Policy No: 1c(1)

OUR LADY'S ABINGDON (OLA)
ONLINE SAFETY POLICY INCLUSIVE OF CYBER BULLYING, ACCEPTABLE USE AND SOCIAL MEDIA

This policy applies to the whole school

This policy, which applies to the whole school, is publicly available on the school website https://www.ola.org.uk/ and upon request a copy may be obtained from the School Office.

Document Details

Information Sharing Category	Public Domain
Version	3
Date Published	September 2022
Authorised by (if required)	Head and the Governing Board
Responsible Area	Leadership Team and Governing Board

We comply with the Government guidance and regulations, currently in force, regarding COVID.

Availability: This policy applies to all members of the OLA community (including staff, pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of OLA's digital technology systems, both in and out of OLA, when working remotely. All new employees and volunteers are required to state that they have read, understood and will abide by this policy and its procedural documents and confirm this by signing the Policies Register.

Monitoring and Review: The online safety policy has been developed by the OLA Whole School Safeguarding Team (WSST) and will be reviewed annually by the safeguarding team who will provide recommendations for updating the policy in the light of experience and changes in legislation or technologies. The School Council will be consulted regarding any changes to the Student AUP. OLA has made a commitment to engage with the 360-degree safe self-review tool as a means of reviewing practice and implementing actions that will improve online safety at OLA.

The implementation of this online safety policy will be monitored by:	*DSL and WSST*
Monitoring will take place at regular intervals:	*September 2022*
The Governing Body will receive a report on the implementation of the online safety policy (which will include anonymous details of online safety incidents) at regular intervals: Online Safety Questions from the Governing Board (Oct 2022)	*By September 2022*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2023*
Should serious online safety incidents take place, the following external persons/agencies should be informed as appropriate, in addition to the DSL:	*OCC Safeguarding Officer, LADO, Police Liaison Officer*

OLA will monitor the impact of the policy when OLA is operating on site and remotely using:

- *Logs of reported incidents*
- *Monitoring logs of internet activity (including sites visited)/filtering (whilst in school)*
- *Internal monitoring data for network activity (whilst in school)*

This document was reviewed and agreed by the Chair of Governors in September 2021.
Signed:

Head	DSL	Chair of Governors
Mr Daniel Gibbons	Chrissi Sharkey	Freddy El Turk
Signed: Daniel Gibbons	Signed: CSharkey	Signed:

Other relevant linked policies:

Online safety is a running and interrelated theme when devising and implementing our wider school policies and procedures, including our *Safeguarding & Child Protection Policy* and our *Preventing Extremism and Tackling Radicalisation Policy.* The staff and student *Acceptable Use Policies (AUPs)* located in the Appendices are central to the Online Safety policy and should be consulted alongside this policy. All staff should read these policies in conjunction with the Online Safety policy. This is particularly important with regard to the Prevent Strategy, as a large portion of cases of radicalisation happen through the online medium. Staff must be vigilant when dealing with such matters and ensure that they observe the procedure for reporting such concerns in line with that laid out in the Safeguarding & Child Protection and Preventing Extremism and Tackling Radicalisation Policies.

- **Safeguarding:** *Safeguarding Children- Child Protection Policy* which includes Sexual Violence and Sexual Harassment (Including Child-on-Child Abuse); *Anti-Bullying Policy*; *Positive Behaviour Code*; *Staff Behaviour (Code of Conduct) Policy*.
- **Prevent Duty:** *Tackling Extremism and Radicalisation Policy*; *Spiritual, Moral, Social and Cultural Development (SMSC); Personal; Personal Social, Health, Economic Education (PSHEE)*; OLA Pupil Expectations (B.A.S.I.C.S)
- *Mobile and Smart Technology Policy*, including taking and storing images of students; *Acceptable use of ICT Sign off forms for Staff/Students; Use of Photographs Sign-off Form.*
- **Health & Safety Policy**
- E-SAFETY AND ICT ACCEPTABLE USE POLICY
- ICT CODE OF CONDUCT FOR STAFF

The following documents have also been consulted.

- Online Safety Bill: Factsheet (Apr 2022)
- Education for a connected world (June 2020)
- Teaching online safety in schools (June 2019)
- Teacher Training Internet Safety and Harms (2020) and Harmful online challenges and online hoaxes (Feb 2021)
- The UK Council for Internet Safety (UKCIS) Online Safety Audit Tool (Oct 2022) – for trainee and ECT teachers
- Online Safety Questions from the Governing Board (Oct 2022)
- Challenging victim blaming language/behaviours when dealing with online experiences of children/young people (Oct 2022)
- Oxfordshire County Council Critical Incidents in Schools Briefing.
- Oxfordshire County Council Domestic abuse and COVID-19
- Oxfordshire County Council E training Safeguarding courses
- Government advice on DBS checks and COVID-19
- Safer Recruitment and Safer Remote Learning
- Templates for online safety and London Grid for Learning – Use of videos and Livestreaming

Legal Status:

- Part 3, paragraphs 7 (a) and (b) of the Education (Independent School Standards) (England) Regulations 2014, in force from the 5th January 2015 and as amended in September 2015
- *Keeping Students Safe in Education* (KCSIE) *Information for all schools and colleges* (DfE: September 2021) incorporates the additional statutory guidance,
- *Disqualification under the Childcare Act 2006 Childcare (Disqualification) and Childcare (Early Years Provision Free of Charge) (Extended Entitlement) (Amendment) Regulations 2018.*
- *Working Together to Safeguard Students* (WT) (HM Government: September 2018) which also refers to non-statutory advice, *Information sharing* HM Government: March 2015); *Prevent Duty Guidance: for England and Wales* (March 2015) (*Prevent*). *Prevent* is supplemented by *The Prevent duty: Departmental advice for schools and childminders (June 2015)* and *The use of social media for on-line radicalisation (July 2015) How Social Media Is Used To Encourage Travel To Syria And Iraq: Briefing Note For Schools (DfE)*
- Based on guidance from the DfE (2014*) 'Cyberbullying: Advice for Heads and School staff* 'and '*Advice for parents and carers on cyberbullying'*

- Prepared with reference to DfE Guidance (2014) *Preventing and Tackling Bullying: Advice for school leaders and governors* and the relevant aspects of *Safe to Learn, embedding anti-bullying work in schools.*
- Having regard for the guidance set out in the DfE *(Don't Suffer in Silence booklet)*
- The Data Protection Act 1998; GDPR, 2018; BECTA and CEOP.
- Teaching Online Safety in School (DfE: 2019)

Section Contents

1. Introduction and scope of policy; Related Documents; Legal Status,
2. Roles and Responsibilities;
3. Breadth and teaching of Online Safety Issues
4. Protecting Personal Data
5. Acceptable use of technology for communications at OLA
6. Radicalisation and the Use of Social Media to Encourage Extremism
7. Cyber-Bullying
8. Online Sexual Harassment
9. Chat Room Grooming and Offline Abuse
10. Social Media, including Facebook, Twitter and Instagram
11. Taking and Storing Images of Students Including Mobile Phones
12 Dealing with unsuitable/inappropriate activities
13 Remote Learning
Appendix 1 – Our Lady's Abingdon (OLA) Student and Parent acceptable use policy
Appendix 2: Our Lady's Abingdon (OLA) Student Acceptable Use Policy – for younger pupils (KS2)
Appendix 3 – Our Lady's Abingdon (OLA) Staff and Volunteer Acceptable Use of ICT Policy
Appendix 4 - Mobile and Smart Technology Policy, including taking and storing images of students
Appendix 5 – Our Lady's Abingdon (OLA) Use of photographs of students and data protection
Appendix 6: Online Safety FAQs
Appendix 7 - Our Lady's Abingdon (OLA) Student Acceptable Use of Mobile Phones and 3G/4G/5G compatible devices
Appendix 8 - Our Lady's Abingdon (OLA) Acceptable Use Agreement for Community Users
Appendix 9 - Challenging victim blaming language and behaviours
Appendix 10: Links to other organisations or documents

1. Introduction and scope of policy:

This Policy covers best practice in the safe use of technology, both on site and in remote learning situations during periods of extended school closure.

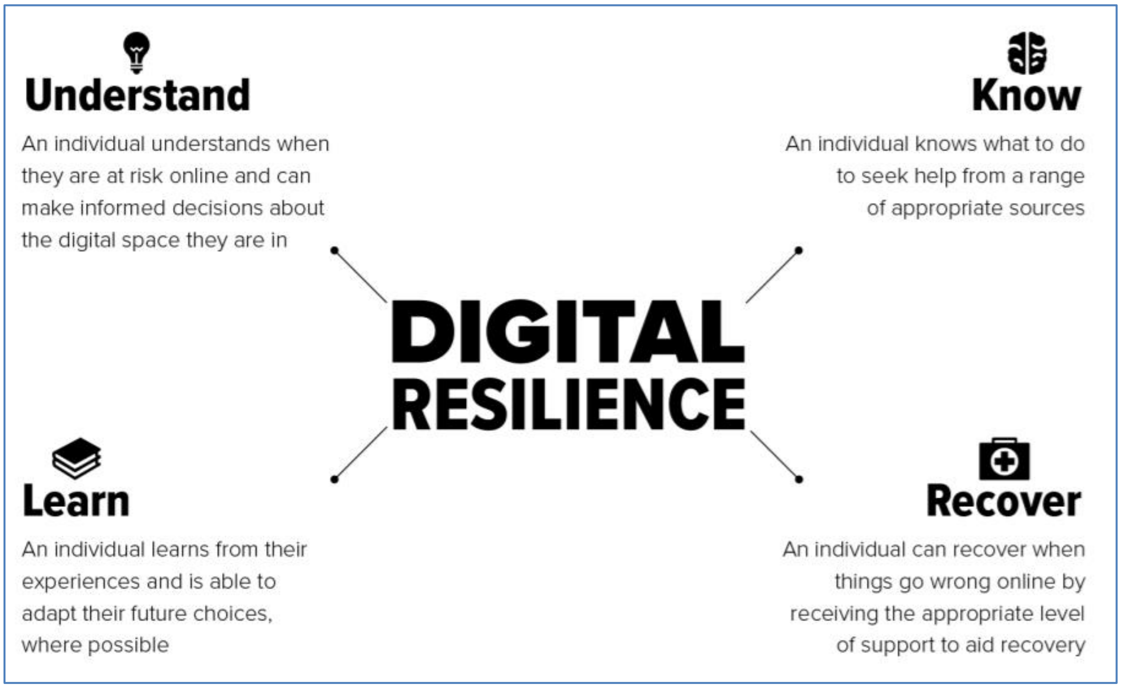
Technology is a big part of everyday life, bringing endless educational and social benefits and opportunities, for adults, children and young people. However, there are potential harms children and young people may encounter when online, including online child abuse, bullying, harassment or criminal exploitation. The consequences and impact of online child abuse can be just as severe as abuse experienced offline. For more information see NSPCC's 2018 report *"Everyone deserves to be happy and safe".*

The purpose of this Policy is to safeguard students and staff at OLA. It details the actions and behaviour required from students and members of staff in order to maintain a safe electronic environment and is based on current best practice drawn from a wide range of sources. In accordance with legislative requirements we have a whole school approach to Online Safety. Our key message to keep students and young people safe is to be promoted and should be applied to both online and offline behaviours. Within our *Online Safety policy*, we have clearly defined roles and responsibilities for online safety as part of the school's wider safeguarding strategy and how this links with our main *Safeguarding & Child Protection Policy* and other related documents.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of pupils when they are off the OLA site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other online safety incidents covered by this policy, which may take place outside of

OLA, but is linked to membership of OLA. **The 2011 Education Act** increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by OLA's Positive Behaviour Code. OLA will deal with such incidents within this policy and associated behaviour, and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that takes place out of school.

We consider how we can promote online safety whilst developing our curriculum, through our staff training, and also through parental engagement.



Understand

An individual understands when they are at risk online and can make informed decisions about the digital space they are in

Know

An individual knows what to do to seek help from a range of appropriate sources

DIGITAL RESILIENCE

Learn

An individual learns from their experiences and is able to adapt their future choices, where possible

Recover

An individual can recover when things go wrong online by receiving the appropriate level of support to aid recovery

UKCIS Digital Resilience Framework

2. Roles and Responsibilities:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about online safety incidents and monitoring reports. A member of the *Governing Board* has taken on the role of *Online Safety Governor*. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead (DSL) as part of WSST meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting back to Governors through Safeguarding and Spiritual Committee.

Head and Leadership Team

- The Head has a duty of care for ensuring the safety (including online safety) of members of the OLA community, though the day to day responsibility will be delegated to the Online Safety Lead (DSL).
- The Head and the DSL should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff *(Flow chart in Appendix).*
- The Head and Chief Operating Officer are responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Head and Deputy Head will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The Leadership Team will receive regular monitoring reports from the DSL

Online Safety Lead (DSL)

Technology provides additional means for safeguarding issues to develop. OLA ensures the DSL is trained in online safety issues and is aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming and online-bullying

During periods of remote learning (such as COVID-19 pandemic): *The DSL remains the primary contact and the Leadership Team and DSL are in regular contact with each other and key members of staff. The Deputies for the various parts of the school will take over should the DSL become unwell. Any incidence of Child-on-Child abuse is reported to the DSL by pupils, parents and staff through the normal channels. If a meeting is required with an individual, then this can be conducted through Zoom or Teams video. In a pandemic situation where staff and pupils are working remotely, it may not be possible to have a trained DSL or deputy available on the OLA site. However, our trained DSL and deputies will be available to be contacted via phone or zoom. All staff are aware of these contact details. The* ***Head*** *will take responsibility for co-ordinating safeguarding on site. Depending on the circumstances, this may include updating and managing access to child protection files, liaising with the offsite DSL (or deputy) and as required liaising with children's social workers where they require access to children in need and/or to carry out statutory assessments at OLA. DSL training is very unlikely to take place for the period COVID-19 measures are in place, however members of the team can take advantage of online training. All OLA staff have had safeguarding training and have read part 1 of KCSIE. Staff are kept informed of any new local arrangements so they know what to do if they are worried about a child. Where new staff are recruited, or new volunteers enter OLA, they are provided with a safeguarding induction. This will include being provided with the updated Child Protection Policy.*

The DSL:

- leads the Online Safety meetings as part of the wider WSST meetings and ensures the importance of online safety in relation to safeguarding is understood by all ICT users.
- takes day to day responsibility for online safety issues with leading role in establishing/reviewing OLA's online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- provides training and advice for staff ; liaises with Oxfordshire County Council and technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety
- meets with Online Safety Governor at WSST to discuss current issues, review incident and filtering/change control logs
- reports regularly to Leadership Team
- incidents dealt with by the Online Safety Lead supported by the Leadership Team and Heads of Section.
- Ensures young people know how to use the Internet responsibly and that parents and teachers have the right measures in place to keep students safe from exploitation or radicalisation.
- Ensures students are safe from terrorist and extremist material when accessing the Internet in school, including by establishing appropriate levels of filtering
- ensures that students use Information and Communications Technology (ICT) safely and securely and are aware of both external and Child-on-Child risks when using ICT, including cyberbullying and other forms of abuse.
- Ensures all staff and volunteers receive appropriate training, guidance, time and resources to effectively implement online safety policies and procedures.
- Ensures the Acceptable Use Policy (AUP) is implemented, monitored and reviewed regularly, and that all updates are shared with relevant individuals at the earliest opportunity.
- Ensures monitoring procedures are transparent and updated as agreed in school policies.
- Ensures allegations of misuse or known incidents are dealt with appropriately and promptly, in line with agreed procedures, and in liaison with other agencies, where applicable.
- Ensures effective online safeguarding support systems are put in place, for example, filtering controls, secure networks and virus protection to ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack.

- Ensures an appropriate level of authorisation is to be given to ICT users. Not all levels of authorisation will be the same - this will depend on, for example, the position, work role and experience of the individual concerned. In some instances, explicit individual authorisation must be obtained for specific activities when deemed appropriate
- Ensures that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- Ensures a current record of all staff and students who are granted access to school ICT system is maintained.

Technical staff

OLA has a managed ICT service provided by an outside contractor. It is the responsibility of OLA to ensure that the managed service provider carries out all the online safety measures that would otherwise be the responsibility of the school technical staff, as suggested below. It is also important that the managed service provider is fully aware of OLA's online safety policy and procedures. Our ICT contractors are also responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

Those with technical responsibilities are responsible for ensuring:

- that OLA's technical systems are managed in ways that ensure that the school meets recommended technical requirements
- that OLA's technical infrastructure is secure and is not open to misuse or malicious attack, with regular reviews and audits of the safety and security of technical systems
- that Servers, wireless systems and cabling are securely located and physical access restricted
- that all users have clearly defined access rights to OLA's technical systems and devices.
- That the "master/administrator" passwords for OLA systems, used by the Network Manager must also be available to the *Head* and kept in a secure place (e.g. a safe)
- that OLA meets required online safety technical requirements and any Oxfordshire County Council online safety policy/guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy
- that all users (at KS3 and above) will be provided with a username and secure password by our ICT engineer who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- the filtering policy is applied and updated regularly and its implementation is not the sole responsibility of any single person
- that they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Head and Leadership Team and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in OLA policies
- that internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes
- that internet filtering/monitoring ensures that children are safe from terrorist and extremist material when accessing the internet.
- That OLA has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users
- That OLA technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement.
- That an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- That appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software.
- That an agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems.

- That an agreed policy is in place regarding the extent of personal use that users (staff/students/pupils/community users) and their family members are allowed on school devices that may be used out of school.
- That an agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- That an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

OLA Online Safety Group (WSST)

The Safeguarding and Online Safety Group (WSST) provides a consultative group that draws in, as necessary, representation from the *OLA* community. It has responsibility for issues regarding online safety and monitoring the Online Safety Policy including the impact of initiatives. The WSST will also be responsible for regular reporting to the Governing Board.

Members of the WSST will assist the DSL with:

- the production/review/monitoring of the school online safety policy/documents.
- the monitoring of the school filtering policy and requests for filtering changes.
- mapping and reviewing the online safety/digital literacy curricular provision – ensuring relevance, breadth and progression
- monitoring network/internet/filtering/incident logs
- consulting stakeholders – including parents/carers and pupils about the online safety provision
- monitoring improvement actions identified through use of the 360-degree safe self-review tool

Teaching and Support Staff (including volunteers)

Access to the Internet and e-mail is provided to support the curriculum, support school administration and for staff professional development only. All staff must read and confirm by signature that they have read the '*Staff Code of Conduct for ICT'* (appendix) before using any school ICT resource. It is the responsibility of all staff to be alert to possible harm to students or staff due to inappropriate internet access or use, both inside and outside of Our Lady's Abingdon, and to deal with incidents of such as a priority.

All staff are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current OLA online safety policy and practices
- they attend updates to Online Safety training.
- they have read, understood and signed the staff acceptable use policy/agreement
- they report any suspected misuse or problem to the Online Safety Lead (DSL) for investigation
- Cyber-bullying incidents will be reported in accordance with OLA's Anti-Bullying Policy
- all digital communications with pupils/parents/carers is on a professional level and only carried out using official OLA systems
- online safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the Online Safety Policy and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students/pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Where students are allowed to freely search the Internet, staff should be vigilant in monitoring the content of the websites the students visit.
- Online Safety issues are embedded in all aspects of the curriculum and other activities.
- If staff allow the use of mobile devices in their lessons, they must ensure that they are used in line with school policy.
- Access to systems should be made by authorised passwords, which must not be made available to any other person.
- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse, using personal data only on secure password-protected computers and other devices. Staff are advised to follow the "How do I stay secure on the Internet?" section in the Online Safety FAQ document.
- Occasionally students may need to research educational material that may normally result in websites being blocked (e.g. racism). In this situation, staff may request to remove these sites form the filtered list for the period of study. Every request to do so should be auditable with clear reasons for the need.

- The Internet can be used to actively gather personal information about individuals which may lead to undesirable consequences (e.g. SPAM, fraud, harassment or identity theft). Because of this, staff are advised to only use the school approved web browsers and email systems which have appropriate security in place. Additionally, files should not be saved directly from the Internet unless they can first be scanned for computer viruses, malware, spyware and other malicious programmes.
- Additionally, staff should not communicate with students through electronic methods such as social networking sites, blogging, chat rooms, texts or private email. Instead, only the school email system should be used for this purpose.
- Educational materials made by and for classes and uploaded to password-protected YouTube channels, i.e. videos of lessons, activities, or fieldtrips, should be logged for record-keeping purposes. This provides an opportunity to share best practices and resources and enable better teaching and learning outcomes.

Any person suspecting another of deliberate misuse or abuse of technology should take the following action:

1. Report in confidence to the DSL.
2. The DSL should investigate the incident.
3. If this investigation results in confirmation of access to illegal material, the committing of illegal acts, or transgression of school rules, appropriate sanctions will be enforced.
4. In exceptional circumstances, where there are reasonable grounds to suspect that a user has committed a serious criminal offence, the CEOP or the police will be informed.
5. No student or member of staff should attempt to access or view the material, whether online or stored on internal or external storage devices. If this step is necessary, CEOP and/or police will be contacted.

During periods of remote learning (such as COVID-19 pandemic): *All OLA staff are aware of the lines of referral. They have access to the Safeguarding poster providing contact details of all members of the Safeguarding team. Staff looking after key worker children have direct lines of contact with DSL or Deputy DSLs. They also have details of all safeguarding agencies such as MASH, should they need to contact them directly. All staff are fully briefed of how to contact DSL and DDSL via email, zoom and telephone. Staff also log any concerns on the Classcharts Safeguarding module. OLA has provided staff, pupils and parents with detailed guidance and reminders about how to behave responsibly online, including the use of Zoom as a video conferencing platform. Any pupil not following the guidelines correctly is being sanctioned in the same way as they would be if they were on site. The DSL is responsible for dealing with any incidents of online misbehaviour.*

Community Users
Community Users who access OLA's systems or programmes as part of the wider school provision will be expected to sign a *Community User Acceptable User Agreement* before being provided with access to school systems.

Parents: Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. OLA will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature.* Parents and carers will be encouraged to support OLA in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website/Learning Platform and on-line student/pupil records
- their children's personal devices in OLA

Pupils:

- are responsible for using OLA's digital technology systems in accordance with the pupil acceptable use agreement
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on online-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that OLA's online safety policy covers their actions out of school, if related to their membership of the school

During periods of remote learning (such as COVID-19 pandemic): *Any incidence of Child-on-Child abuse is reported to the DSL by pupils, parents and staff through the normal channels. If a meeting is required with an individual, then this can be conducted through Zoom or Teams video.*
Attendance*: Pupils are expected to register during remote learning as normal; AM and PM with their tutor and lesson-by-lesson. OLA has an up to date list of key worker children and is providing on site daily supervision for key worker and vulnerable children. OLA will also follow up with any parent or carer who has arranged care for their children within the school and the children subsequently do not attend. OLA performs an annual data check to ensure that emergency contact numbers are correct. In all circumstances where a vulnerable child does not take up their place with OLA, or discontinues, their social worker is contacted.*
Vulnerable children *include those who have a social worker and those children and young people up to the age of 25 with EHC plans. Local authorities have the key day-to-day responsibility for delivery of children's social care. Social workers and VSHs will continue to work with vulnerable children in remote learning and should support these children to access this provision. There is an expectation that children with a social worker will attend provision, unless in consultation with the child's social worker and family it is agreed this is not in the best interests of the child. During remote learning, the DSL (and deputies) at OLA know who the most vulnerable children are and have the flexibility to offer a place to those on the edges of receiving children's social care support. OLA will continue to work with and support children' social workers to help protect vulnerable children. This will be especially important during the COVID-19 period.*

3. Breadth and teaching of Online Safety Issues:

We classify the issues within online safety into **four** areas of risk which are managed by reducing availability, restricting access, and promoting safe and responsible use.

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: Child-on-Child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

- **Commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams.

Teaching about online safety: Because new opportunities and challenges appear all the time, it is important that we focus our teaching on the underpinning knowledge and behaviours that can help pupils to navigate the online world safely and confidently regardless of the device, platform or app. Online Safety is a focus in all areas of the curriculum and key online safety messages are reinforced regularly, teaching students about the risks of Internet use, how to protect themselves and their peers from potential risks, how to recognise suspicious, bullying or extremist behaviour and the consequences of negative online behaviour. Access levels to ICT reflect the curriculum requirements and age of students. Staff should guide students to on-line activities that will support the learning outcomes planned for the students' age and maturity. This teaching is built into existing lessons alongside our wider whole-school approach.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum is provided as part of Computing/PHSE/other lessons and is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and pastoral activities. *Prior to periods of remote learning, assemblies are used for this purpose.*
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.

- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Pupils are helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside OLA.
- Staff act as good role models in use of digital technologies, the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Students will explicitly be taught the following topics through their lessons:

- What internet use is acceptable and what is not and given clear guidelines for internet use;
- How to use a wide range of devices and learn about their advantages and disadvantages, in different applications;
- How to evaluate what they see online;
- How to recognise techniques used for persuasion;
- Online behaviour;
- How to identify online risks and
- How and when to seek support.

We recognise that Child-on-Child abuse can occur online and to this end we teach students how to spot early warning signs of potential abuse, and what to do if students are subject to sexual harassment online. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, eg involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

Victim blaming: Current *UK Council for Internet Safety (UKCIS) guidance* (Oct 2022) highlights that victim blaming is any language or action that implies (whether intentionally or unintentionally) that a person is partially or wholly responsible for abuse that has happened to them. It is harmful and can wrongfully place responsibility, shame or blame onto a victim, making them feel that they are complicit or responsible for the harm they have experienced. People of all ages can display victim blaming attitudes and it can happen both online and offline. Education professionals are encouraged to think critically about the language they use and the impact that it has, both in the moment and more widely across society.

Blaming children and young people for their own abuse is never acceptable. Professionals should clearly understand that children can never be expected to predict, pre-empt or protect themselves from abuse. Irrespective of the context or circumstance, the responsibility always lies with the person who abused the child or young person. One of the greatest barriers to a child or young person seeking help and reporting online abuse, is feeling they are to blame for something that has happened to them. When professionals working with the child or young person speak or behave in such a way that reinforces this feeling of self-blame, the impact of the abuse the child or young person has already experienced may be greater, leading to a longer recovery.

When victim blaming occurs, there is a risk of diminishing the child or young person's experiences, leading to a lack of, or an inappropriate, safeguarding response. This could be by professionals initially dealing with an incident or by those involved subsequently. This can have a devastating impact for the child or young person who has experienced abuse and make it less likely that they, or their peers, will have the confidence to disclose abuse in the future. In addition, victim blaming attitudes can prevent families, friends and wider society from recognising certain behaviours as abuse.

Language and behaviour that implies that a child or young person is complicit in, or responsible in some way, for any harm or abuse they've experienced or may experience is victim blaming. **See Appendix 9.**

Direct victim blaming happens when a child or young person is explicitly held responsible for what has happened to them.
Examples:

- In the context of non-consensual nude image sharing, professionals may blame the child or young person for sharing the image in the first place, and say what's happening to them is their fault because they sent the image
- After receiving an abusive message online, a professional may say it's the child or young person's fault for accepting a friend request from someone they didn't know on social media.
- After being bullied through an online game, a professional decides not to take any action because they think the child or young person is partly to blame for playing an online game with a minimum age requirement that is older than they are.
- In the context of online blackmail, a professional tells a child or young person they should not have responded, but blocked and reported the person as soon as they started sending threatening messages.

Indirect or unintentional victim blaming can be harder to identify. It often happens when a person is trying to help a child or young person after something has happened to them. However, that 'help' reinforces the idea that the child or young person has done something wrong or is responsible for what has happened to them.
Examples:

- Taking away the child or young person's device or banning them from using an online platform, app or game as a consequence.
- Delivering online safety education to a child or young person immediately after a disclosure, which highlights what they should have done to keep themselves safe.
- Inferring or suggesting that a child or young person should take responsibility for keeping themselves safe online.
- When speaking to the child or young person after a disclosure, telling them what they should have done differently in that situation in order to keep themselves safe.

Educating Students: Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety/digital literacy is therefore an essential part of the school's online safety provision and is vital during periods of remote learning. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

In relation to remote learning (*as outlined in COVID-19: Safeguarding in schools, Colleges and other providers*), the following important safeguarding principles remain the same:

- the best interests of OLA children must always continue to come first
- if anyone in OLA has a safeguarding concern about any child they should continue to act immediately
- the DSL or deputy should be available
- it is essential that unsuitable people are not allowed to enter OLA and/or gain access to children
- children should continue to be protected when they are online

All OLA students must agree to the IT Acceptable Use Policy before accessing the school systems. Students will be given supervised access to our computing resources and will be provided with access to filtered Internet (see FAQ Document) and other services.

Problems with ICT equipment should be reported either to the Class Teacher (Lower School) or directly to the IT technician (Senior School) using the email: support@planet-it.net . The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of students and young people. OLA will ensure that the use of Internet-derived materials by staff and students complies with copyright law. OLA will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our Personal, Social, Health and Economic Education (PSHEE) and Spiritual, Moral, Social and Cultural (SMSC) Development. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

Educating Staff: A planned calendar programme of online safety training opportunities will be available to all staff members. Staff will be provided with sufficient Online Safety training to protect students and themselves from online risks and to deal appropriately with Online Safety incidents when they occur. Ongoing staff development training includes training in online safety, together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles and requirements. Staff will undergo online safety training annually/when changes occur, to ensure they are aware of current online safety issues and any changes to OLA's provision for online safety, as well as current developments in social media and the internet as a whole.

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the OLA's online safety policy and acceptable use agreements.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The DSL will provide advice/guidance/training to individuals as required.

All staff will employ methods of good practice and act as role models for young people when using the internet and other digital devices. All staff will be educated on which sites are deemed appropriate and inappropriate. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism. Any new staff are required to undergo online safety training as part of their induction programme, ensuring they fully understand this online safety policy/social media policy/user agreement. The DSL will act as the first point of contact for staff requiring online safety advice.

During periods of remote learning (such as COVID-19 pandemic):
With regard to safer recruitment/volunteers and movement of staff*: As OLA continues to recruit new staff, we will continue to follow the relevant safer recruitment processes, including, as appropriate, relevant sections in part 3 of KCSIE. In response to COVID-19, the Disclosure and Barring Service (DBS) has made changes to its guidance on standard and enhanced DBS ID checking to minimise the need for face-to-face contact. Where OLA is utilising volunteers, we will continue to follow the checking and risk assessment process as set out in paragraphs 167 to 172 of KCSIE. Under no circumstances will a volunteer who has not been checked be left unsupervised or allowed to work in regulated activity.*

At the present time, OLA does not have any staff members engaged in temporary regulated activity within another school to support the care of children. However, we understand that there is no expectation that a new DBS check should be obtained for the new school setting. The type of setting on the DBS check, for example a specific category of school, is not a barrier. The same principle applies if childcare workers move to work temporarily in a school setting. The receiving institution should risk assess as *they would for a volunteer. Whilst the onus remains on schools to satisfy themselves that someone in their setting has had the required checks, including as required those set out in part 3 of KCSIE, in the above scenario this can be achieved, if the receiving institution chooses to, via seeking assurance from the current employer rather than requiring new checks.*

OLA will continue to follow our legal duty to refer to the DBS anyone who has harmed or poses a risk of harm to a child or vulnerable adult. Full details can be found at paragraph 163 of KCSIE. OLA will continue to consider and make referrals to the Teaching Regulation Agency (TRA) as per paragraph 166 of KCSIE and the TRA's 'Teacher misconduct advice for making a referral. During the COVID-19 period all referrals should be made by emailing Misconduct.Teacher@education.gov.uk. All referrals received by the TRA will continue to be considered. Where referrals on serious safeguarding matters are received and it is deemed that there is a public interest in doing so consideration will be given as to whether an interim prohibition order (IPO) should be put in place. The TRA will continue to progress all cases but will not schedule any hearings at the current time. OLA is aware, on any given day, which staff/volunteers will be on site, and we will ensure that appropriate checks have been carried out, especially for anyone engaging in regulated activity. We will continue to keep the single central record (SCR) up to date as outlined in paragraphs 148 to 156 in KCSIE. We are aware that the SCR can, if OLA chooses, provide the means to log everyone that will be working or volunteering in a school or college on any given day, including any staff who may be on loan from other institutions. The SCR can also, if a school or college chooses, be used to log details of any risk assessments carried out on volunteers and staff on loan from elsewhere.

***With regard to mental health of pupils through increased online activity:** Negative experiences and distressing life events, can affect the mental health of pupils and their parents. OLA staff are aware of this in setting expectations of pupils' work where they are at home. Where providing for children of critical workers and vulnerable children on site, OLA has ensured that appropriate support is in place for them. Mental health issues can bring about changes in a young person's behaviour or emotional state which can be displayed in a range of different ways, and that can be an indication of an underlying problem. Support for pupils and students at OLA during remote learning is provided by:*

- *regular check-ins from Heads of Section*
- *online wellbeing questionnaires*
- *follow up on low questionnaire scores by pastoral team*
- *Guidance information distributed to parents through connectED parent resource*
- *Guidance information distributed to staff through connectED staff resource*
- *'Feel Good Friday' activities (drawing upon the guidance supplied in mental health and behaviour in schools.)*

Educating Governors: The Governing Board should take part in online safety training/awareness sessions, with particular importance for those who are members of the OLA WSST. This may be offered in a number of ways:

- Attendance at training provided by the OCC/National Governors Association
- Participation in OLA training sessions for staff or parents
- Technical – infrastructure/equipment, filtering and monitoring

Educating Parents/Guardians: We believe that it is essential for parents/carers to be fully involved with promoting Online Safety both in and outside of school and to be aware of their responsibilities. Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

- We regularly consult and discuss Online Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks. For example, Parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on School website).
- Parents are provided with a copy of the *Pupil IT Acceptance Policy*, and parents are asked to sign it, as well as students age eight and older.

- We organise an annual awareness session for parents with regards to Online Safety which looks at emerging technologies and the latest ways to safeguard students from inappropriate content.
- OLA will seek to provide information and awareness to parents and carers through:
  - *Curriculum activities*
  - *Letters, newsletters, web site, Learning Platform*
  - *Parents evenings; High profile events/campaigns e.g. Safer Internet Day*
  - *Reference to the relevant web sites/publications e.g.* swgfl.org.uk, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers *(see appendix for further links/resources)*

Parents and guardians are always welcome to discuss their concerns on Online Safety with the school, who can direct them to the support of our DSL if required. Parents and carers are encouraged to support OLA in promoting good Online Safety practice.

Educating the Wider Community: OLA will provide opportunities for local community groups/members of the community to gain from OLA's online safety knowledge and experience. This may be offered through the following:

- *Providing family learning courses in use of new digital technologies, digital literacy and online safety*
- *Online safety messages targeted towards grandparents and other relatives as well as parents.*
- *OLA's website will provide online safety information for the wider community*
- *Sharing online safety expertise/good practice with other local schools*
- *Supporting community groups e.g. Early Years Settings, Childminders, youth/sports/voluntary groups to enhance their online safety provision*

4. Protecting Personal Data:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2018. OLA recognises that if required, data may need to be obtained by relevant parties such as the Police. Students are encouraged to keep their personal data private as part of our Online Safety lessons and IT curriculum, including areas such as password protection and knowledge about apps and unsecured networks/apps etc. OLA is responsible for ensuring we have an appropriate level of security protection procedures in place, in order to safeguard systems, staff and learners and we review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies.

OLA will ensure that:

- it has a Data Protection Policy
- it implements the data protection principles and is able to demonstrate that it does so through policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of Data Protection Officer (DPO).
- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for. The school should develop and implement a 'retention policy" to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how OLA looks after their data and what their rights are in a clear Privacy Notice

- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply).
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- data must be encrypted and password protected.
- device must be password protected.
- device must be protected by up to date virus and malware checking software
- data must be securely deleted from the device, in line with OLA's policy once it has been transferred or its use is complete.

Staff will ensure that they:

- at all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the school
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- will not transfer any OLA personal data to personal devices except as in line with school policy
- access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data

***For any children moving schools during the COVID-19 pandemic**, the DSL will provide the receiving institution with any relevant welfare and child protection information. This will be especially important where children are vulnerable. For looked-after children, any change in school should be led and managed by the VSH with responsibility for the child. The receiving institution should be aware of the reason the child is vulnerable and any arrangements in place to support them. As a minimum the receiving institution should, as appropriate, have access to a vulnerable child's EHC plan, child in need plan, child protection plan or, for looked-after children, their personal education plan and know who the child's social worker (and, for looked-after children, who the responsible VSH is). This should ideally happen before a child arrives and, where that is not possible as soon as reasonably practicable. In the event that the SENCo is unable to work, the DSL (or Deputy) should take responsibility for any paperwork. Whilst schools and colleges must continue to have appropriate regard to data protection and GDPR they do not prevent the sharing of information for the purposes of keeping children safe*

5. Acceptable use of technology for communications at OLA:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following shows how OLA currently considers the benefit of using these technologies whilst in school for education:

	Staff & other adults				*Students/Pupils*			
Communication Technologies	**Allowed**	**Allowed at certain times**	**Allowed for selected staff**	**Not allowed**	**Allowed**	**Allowed at certain times**	**Allowed with staff permission**	**Not allowed**
Mobile phones may be brought to OLA					•			
Use of mobile phones in lessons								•
Use of mobile phones in social time								•
Taking photos on mobile phones/cameras								•
Use of other mobile devices e.g. tablets, gaming devices								•
Use of personal email addresses in OLA, or on school network								•
Use of school email for personal emails		•				•		
Use of messaging apps	•							•
Use of social media	•							•
Use of blogs	•							•

When using communication technologies, OLA considers the following as good practice:

- The official OLA email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and pupils should therefore use only the OLA email service to communicate with others when in school, or on OLA systems (e.g. by remote access).
- Users must immediately report, to the nominated person – in accordance with OLA policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and pupils or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) OLA systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class/group email addresses may be used at KS2, in addition to individual OLA e-mail addresses for Teams use, while pupils at KS3 and above will be provided with individual OLA email addresses for educational use.
- Pupils should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.
- Personal information should not be posted on the OLA website and only official email addresses should be used to identify members of staff.

Use of Email

- The use of personal email accounts to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other young persons, staff or third parties via works email.
- Yong people are made aware that all email messages are monitored and that the filtering system will detect inappropriate links, viruses, malware and profanity.
- Staff members are aware that their email messages may be monitored.
- Any emails sent by young people to external organisations will be overseen by their teacher/support worker and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

Mobile Electronic Devices (Phones, Laptops, iPads and Tablets):

OLA does not have a BYOD Policy and does not supply devices to pupils, although Microsoft Surface devices are planned for the future. Mobile technology devices will therefore be personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage. All users should understand that the use of mobile/personal devices within school is prohibited. Whilst working remotely, pupils will have greater access to mobile technology and for extended periods of time, than they would have whilst on site in school. Teaching about the safe and appropriate use of mobile technologies is an integral part of the OLA's online safety education programme. OLA's acceptable use agreements for staff, pupils and parents/carers considers the use of mobile technologies

Mobile telephones are not permitted to be used whilst in the academic school buildings. During the school day phones are only to be used by students during break time and lunch time (KS3 onwards). Mobile phones are kept on site at the risk of the individual student - OLA is not responsible for any devices lost or damaged whilst on school grounds. If in the rare case a student in KS2 brings a mobile phone into lessons, this must be passed onto the office to store until the end of the day. In KS3 and upwards, students must ensure that their devices are kept in a secure place, e.g. their school bag or in their locker.

Using the camera on a phone or similar device, either to photograph/film/record any member of the OLA community, do any form of live streaming or to show to others the photos/videos/audio recordings already on the phone or similar device is prohibited. The discovery of any uploads to social media platforms will result in serious sanctions being applied.

OLA is committed to providing a safe environment, including online.

OLA follows the guidance issued and has appropriate filtering and monitoring mechanisms in place, to protect children when they are online on the school or college's IT systems or recommended resources. The UK Council for Internet Safety provides information to help governing boards and proprietors assure themselves that any new arrangements continue to effectively safeguard children online. The UK Safer Internet Centre's professional online safety helpline also provides support for the children's workforce with any online safety issues they face. Local authorities may also be able to provide support.

Our use of online learning tools and systems is in line with privacy and GDPR requirements. Advice given to staff on remote learning follows the same principles as set out in OLA's staff code of conduct (acceptable use of technologies, staff pupil/student relationships and communication including the use of social media). An appendix has been added to the Code of Conduct to cover the period of COVID-19. Advice given to pupils follows the same principles as stated in our Positive Behaviour Code. In all remote learning communications with parents, the importance of children being safe online has been reinforced. An essential part of the online planning process will be ensuring children who are being asked to work online have very clear reporting routes in place so they can raise any concerns whilst online. As well as reporting routes back to the school or college this should also signpost children to age appropriate practical support from the likes of:

- Childline - for support
- UK Safer Internet Centre - to report and remove harmful online content
- CEOP - for advice on making a report about online abuse

Where parents and carers choose to supplement the school's online offer with support from online companies and in some cases individual tutors, the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and can be trusted to have access to children, has been reinforced.

Support for parents and carers to keep their children safe online includes:

- Internet matters - for support for parents and carers to keep their children safe online
- London Grid for Learning - for support for parents and carers to keep their children safe online
- Net-aware - for support for parents and careers from the NSPCC
- Parent info - for support for parents and carers to keep their children safe online
- Thinkuknow - for advice from the National Crime Agency to stay safe online
- UK Safer Internet Centre - advice for parents and carers

6. Radicalisation and the Use of Social Media to Encourage Extremism:

The Internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs, sharing extreme ideological views or advocating the use of violence to solve problems. This has led to social media becoming a platform for:

- Intensifying and accelerating the radicalisation of young people;
- Confirming extreme beliefs;
- Accessing likeminded people where they are not able to do this off-line, creating an online community;
- Normalising abnormal views and behaviours, such as extreme ideological views or the use of violence to solve problems and address grievances.

OLA has a number of measures in place to help prevent the use of social media for this purpose:

- Web site filtering is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or Twitter by students.
- Students, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found in guidance from the Department for Education '*How Social Media Is Used to Encourage Travel to Syria and Iraq: Briefing Note for Schools.'*

Reporting of Online Safety Issues and Concerns Including Concerns Regarding Radicalisation:

OLA has clear reporting mechanisms in place, available for all users to report issues and concerns. For staff, any concerns regarding Online Safety should be made to the DSL, who will review the issue and take the appropriate action. For students, they are taught to raise any concerns to their class teacher (Lower School) or Form Tutor/Head of Section, who will then pass this on to the DSL. Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy.

Our DSL provides advice and support to other members of staff on protecting students from the risk of on-line radicalisation. We ensure staff understand what radicalisation and extremism mean and why people may be vulnerable to being drawn into terrorism. We ensure staff have the knowledge and confidence to identify students at risk of being drawn into terrorism, and to challenge extremist ideas, which can be used to legitimise terrorism. Staff safeguard and promote the welfare of students and know where and how to refer students and young people for further help as appropriate by making referrals as necessary to Channel.

Assessing Risks:

- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the OLA network. OLA cannot accept liability for any material accessed, or any consequences of Internet access.
- Developing technologies, such as mobile phones with Internet access are not governed by the school's infrastructure and can bypass any and all security and filtering measures that are or could be deployed. We recognise the additional risks this has for our students, who could have unsupervised access to the internet when using their own devices in their free time. To address

this, the school works with pupils across our age range to ensure that students are educated clearly about the risks of both social media and internet use, alongside regularly monitoring of device usage as appropriate.

- We will audit ICT use to establish if the Online Safety policy is sufficiently robust and that the implementation of the Online Safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The Governing Board will review and examine emerging technologies for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Any person not directly employed by the school will not be provided with access to any of the school systems with the exception of filtered *Wi-Fi* access.
- OLA takes measures to ensure appropriate IT filters monitoring systems are in place to safeguard students from potentially harmful and inappropriate material on-line without unreasonable “over-blocking”
- The school recognises that students may choose to circumvent certain safety precautions by using mobile data on their devices over 3G, 4G and 5G. To help provide a safe environment for all students, we will supplement the systems filtering with behaviour management and additional staff/student training.

7. **Cyber-Bullying:** is the use of ICT, particularly mobile electronic devices and the Internet, deliberately to upset someone else. Cyberbullying (along with all forms of bullying) will not be tolerated and incidents of cyberbullying should be reported and will be dealt with in accordance with OLA’s Anti-Bullying Policy. Use of electronic devices of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline. If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under OLA's child protection procedures (see our Safeguarding & Child Protection Policy). Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- **Chat room bullying and online grooming** involve sending menacing or upsetting responses to students or young people when they are in a web-based chat room;
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages through various messaging applications (for example, WhatsApp, Group Me, Skype, Facebook Messenger, Snapchat, Google Hangouts etc.) as they conduct real-time conversations online;
- **Bullying via websites and social networks (an example of this would be Facebook, Twitter, Instagram, etc.)** includes the use of defamatory blogs, personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Students should remember the following:

- Always respect others - be careful what you say online and what images you send.
- Think before you send - whatever you send can be made public very quickly and could stay online forever.
- Don't retaliate or reply online.
- Save the evidence - learn how to keep records of offending messages, pictures or online conversations. Ask someone if you are unsure how to do this. This will help to show what is happening and can be used by the school to investigate the matter.
- Block the bully. Most social media websites and online or mobile services allow you block someone who is behaving badly.
- Don't do nothing - if you see cyberbullying going on, support the victim and report the bullying.

8. Online Sexual Harassment:

Sexual harassment creates an atmosphere that, if not challenged, can normalise inappropriate behaviours and provide an environment that may lead to sexual violence. Online sexual harassment includes: non-consensual sharing of sexual images and videos and sharing sexual images and videos (both often referred to as sexting); inappropriate sexual comments on social media; exploitation; coercion and threats. Online sexual harassment may be standalone, or part of a wider pattern of sexual harassment and/or sexual violence. All cases or allegations of sexual harassment, online or offline, is unacceptable and will dealt with under our Child Protection Procedures.

Additionally, we recognise that incidents of sexual violence and sexual harassment that occur online (either in isolation or in connection to offline incidents) can introduce a number of complex factors. These include the potential for the incident to take place across a number of social media platforms and services and for things to move from platform to platform online. It also includes the potential for the impact of the incident to extend further than the school's local community (e.g. for images or content to be shared around neighbouring schools/colleges) and for a victim (or alleged perpetrator) to become marginalised and excluded by both online and offline communities. There is also the strong potential for repeat victimisation in the future if abusive content continues to exist somewhere online. Online concerns can be especially complicated. Support is available at:

a. The UK Safer Internet Centre provides an online safety helpline for professionals at 0344 381 4772 and helpline@saferinternet.org.uk. Providing expert advice and support for school staff with regard to online safety issues and when an allegation is received.
b. If the incident involves sexual images or videos that have been made and circulated online, we will support the victim to get the images removed through the Internet Watch Foundation (IWF). The IWF will make an assessment of whether the image is illegal in line with UK Law. If the image is assessed to be illegal, it will be removed and added to the IWF's Image Hash list.

ICT-Based Sexual Abuse (Including Sexting): The impact on a child of ICT-based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT-based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family. All adults (volunteers, staff) working with students, adults and families will be alerted to the possibility that:

- A child may already have been/is being abused and the images distributed on the Internet or by mobile telephone;
- An adult or older child may be grooming a child for sexual abuse, including involvement in making abusive images. This process can involve the child being shown abusive images;
- An adult or older child may be viewing and downloading child sexual abuse images.

Pupils are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. The school will treat incidences of sexting (both sending and receiving) as a safeguarding issue and pupils concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

There are no circumstances that will justify adults possessing indecent images of students. Adults who access and possess links to such websites will be viewed as a significant and potential threat to students. Accessing, making and storing indecent images of students is illegal. This will lead to criminal investigation and the individual being barred from working with students, if proven. Adults should not use equipment belonging to the school to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with students. Adults should ensure that students are not exposed to any inappropriate images or web links. Where indecent images of students or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Adults should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated, which in itself can lead to a criminal prosecution.

Sanctions: Sanctions will depend on the severity of the offence as assessed by the Leadership Team. They may include one or more of the following:

- Temporary or permanent ban on the use of ICT resources in the School.
- Temporary or permanent ban on the use of the Internet in the School.
- Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour.
- Temporary or permanent exclusion from school may be imposed.
- If appropriate, police or local authorities may be involved.

9. **Chat Room Grooming and Offline Abuse:** Our staff need to be continually alert to any suspicious activity involving computers and the Internet. Grooming of students online is a faster process than usual grooming, and totally anonymous. The abuser develops a 'special' relationship with the child online (often adopting a false identity), which remains a secret to enable an offline meeting to occur in order for the abuser to harm the child.

10. Social Media, including Facebook, Twitter and Instagram:

Facebook, Twitter, Instagram and other forms of social media are increasingly becoming an important part of our daily lives, including part of the school's marketing strategy.

Social Media - Protecting Professional Identity: All schools and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render OLA or Oxfordshire County Council liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

OLA provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

OLA staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or OLA staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to OLA or OCC
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information
- They do not access their personal social media accounts using school equipment at any time, unless granted prior permission by the Head for reasons of work
- They follow advice not to befriend or follow parents of students and to keep their personal profile as private as possible
- They follow information on how to use social media responsibly and what to do if they are aware of inappropriate use by others
- They are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever

When official OLA social media accounts are established there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under OLA's disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with OLA or impacts on OLA, it must be made clear that the member of staff is not communicating on behalf of OLA with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- OLA permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media: OLA's use of social media for professional purposes will be checked regularly by the senior risk officer and Online Safety Group to ensure compliance with the school policies.

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school
- The school should effectively respond to social media comments made by others according to a defined policy or process

Behaviour

- OLA requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. OLA social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.
- If a journalist makes contact about posts made using social media staff must follow the school media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by OLA and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with OLA policies. *The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken*
- The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, OLA will deal with the matter internally. Where conduct is considered illegal, OLA will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Staff and students are aware that their online behaviour should at all times be compatible with UK law. Additionally, more information on best practice for staff can be found in our Staff Behaviour (Code of Conduct) Policy. OLA recognises that Social media is very likely to play a central role in the fall out from any incident or alleged incident. There is the potential for contact between victim and alleged perpetrator and a very high likelihood that friends from either side could well harass the victim or alleged perpetrator online.

11. Taking and Storing Images of Students Including Mobile Phones (See our related documents including Appendix 3):

OLA provides an environment in which students, parents and staff are safe from images being recorded and inappropriately used. Upon their initial visit, parents, volunteers and visitors are given information informing them they are not permitted to use mobile phones on the premises in the presence of students, or to take photographs of students apart from circumstances as outlined in Appendix 6 of this policy. This prevents staff from being distracted from their work with students and ensures the safeguarding of students from inappropriate use of mobile phone cameras and other digital recording equipment. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images of themselves and others especially on social networking sites.
- Photographs published onto any website will comply with good practice guidance on the use of such images. Care will be taken to ensure that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. Their full names will not be used anywhere in the website, particularly in association with photographs.

N.B. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc. The school has a Mobile Phone section in the Staff Behaviour Policy, which includes:

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Our Lady's Abingdon, taking into consideration staff, students on placement, volunteers, other professionals, visitors and parents/carers.
- How we inform parents/carers, visitors and other professionals of our procedures.
- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. OLA will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on OLA's website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at OLA events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow OLA policies concerning the sharing, distribution and publication of those images. Those images should only be taken on OLA equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or OLA into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Sending or posting of nude or semi-nude images (see Gov guidelines here)

In the latest advice for schools and colleges (UKCIS, 2020), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. This could be via social media, gaming platforms, chat apps or forums. It could also involve sharing between devices via services like Apple's Air Drop which works offline. Alternative terms used by children and young people may include 'dick pics' or 'pics'.

The motivations for taking and sharing nude and semi-nude images, videos and live streams are not always sexually or criminally motivated. This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. Your setting's child protection policy should outline codes of practice to be followed.

Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.

If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.

Do not delete the imagery or ask the young person to delete it.

Do not ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).

Do not share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.

Do not say or do anything to blame or shame any young people involved.

Do explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

12. Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from OLA and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school context, either because of the age of the users or the nature of those activities.

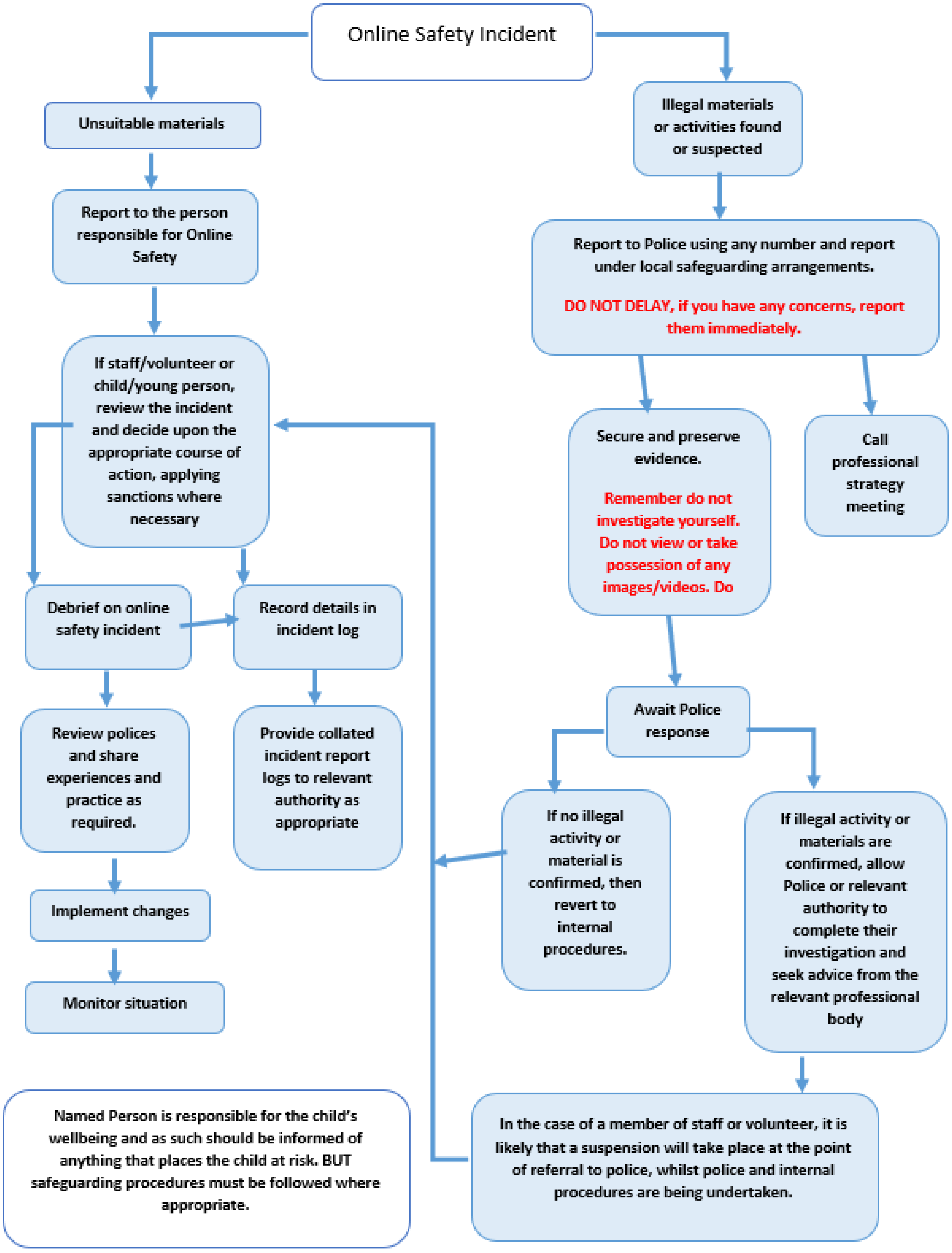
OLA believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in/or outside OLA when using OLA equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks,	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. OLA refers to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

proposals or comments that contain or relate to:	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)						X
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)					X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)					X	
Using school systems to run a private business					X	
Infringing copyright					X	
On-line gaming (educational)			x			
On-line gaming (non-educational)					x	
On-line gambling					x	
On-line shopping/commerce					x	
File sharing		x				
Use of social media					x	
Use of messaging apps					x	
Use of video broadcasting e.g. Youtube					x	

Responding to incidents of misuse: This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “User Actions” above).

Illegal Incidents: If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the Flowchart (below) for responding to online safety incidents and report immediately to the police.


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

Other Incidents

It is hoped that all members of the OLA community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by OCC or national/local organisation (as relevant).
    - Police involvement and/or action

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- offences under the Computer Misuse Act (see User Actions chart above)
- other criminal conduct, activity or materials

Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.
It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School actions & sanctions
It is more likely that OLA will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

	Actions/Sanctions								
Students/Pupils Incidents	Refer to class teacher/tutor	Refer to Head of Department/Year/other	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons									
Unauthorised/inappropriate use of mobile phone/digital camera/other mobile device									
Unauthorised/inappropriate use of social media/ messaging apps/personal email									
Unauthorised downloading or uploading of files									
Allowing others to access school network by sharing username and passwords									
Attempting to access or accessing the school network, using another pupil's account									
Attempting to access or accessing the school network, using the account of a member of staff									
Corrupting or destroying the data of other users									
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature									
Continued infringements of the above, following previous warnings or sanctions									
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school									
Using proxy sites or other means to subvert the school's filtering system									

Accidentally accessing offensive or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material									
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act									

	Actions/Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher Principal	Refer to Local Authority/HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).		X	X	X				
Inappropriate personal use of the internet/social media/personal email								
Unauthorised downloading or uploading of files								
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account								
Careless use of personal data e.g. holding or transferring data in an insecure manner								
Deliberate actions to breach data protection or network security rules								
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software								
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature								
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students/pupils								
Actions which could compromise the staff member's professional standing								
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school								

Using proxy sites or other means to subvert the school's filtering system								
Accidentally accessing offensive or pornographic material and failing to report the incident								
Deliberately accessing or trying to access offensive or pornographic material								
Breaching copyright or licensing regulations								
Continued infringements of the above, following previous warnings or sanctions								

13. Remote Learning (Please see our Remote Learning Policy for more details):

Where there are periods in which the school is forced to close, yet continue to provide education (such as during the COVID-19 Pandemic) it is important that OLA supports staff, students and parents to access learning safely, especially considering the safety of our vulnerable students. Staff and volunteers are aware that this difficult time potentially puts all children at greater risk and the school recognises the importance of all staff who interact with children, including online, continuing to look out for signs a child may be at risk. Staff and volunteers will continue to be alert to any signs of abuse, or effects on learners' mental health that are also safeguarding concerns, and will act on concerns immediately. Any such concerns should be dealt with as per the Child Protection Policy and where appropriate referrals should still be made to children's social care and as required, the police. Online teaching should follow the same principles as set out in the school's staff and pupils respective Behaviour - Code of Conducts. Additionally, school name will ensure any use of online learning tools and systems is in line with privacy and data protection/GDPR requirements.

OLA will put additional measures in place to support parents and students who are learning from home. This will include specific guidance on which programmes OLA is expecting students to use and how to access these alongside how students and parents can report any concerns that they may have. Guidance will also be issued on which staff members students will have contact with and how this will happen, including how to conduct virtual lessons (including video conferencing). Details of this can be found in our Remote Learning Policy.

Additionally, the Head has a duty of care for ensuring the safety (including online safety) of members of the school community, with the day to day responsibility being delegated to the Online Safety Lead who is our DSL. The Head and the DSL are aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff, which in line with our main safeguarding reporting procedures.

Staff working remotely should wherever possible use their school-issued ICT equipment, however they may use their own computer equipment if this is not practical, as long as it is in accordance with the school's Data Protection Policy. Staff are responsible for security of personal data and must ensure it is stored securely when using personal systems or remote systems to maintain confidentiality from other members of the household.

For more information relating to Online Safety procedures, refer to the Online Safety Frequently Asked Questions (FAQ) in Appendix 5. It covers the following topics on the relevant page as follows:

1 How will the policy be introduced to students? How will staff be consulted and made aware of this policy? How will complaints regarding Internet use be handled? How will parents' support be enlisted?
2 Why is the use of Internet and ICT important? How is the safe use of ICT and the Internet promoted? How does the Internet and use of ICT benefit education in our school? How will students learn to evaluate Internet content?
3 How is filtering managed? How are emerging technologies managed? How to react to misuse by students and young people
4 How is printing managed? What are the categories of Cyber-Bullying? What are the student rules?

5 What has research into Cyber Bullying found? What is the impact on a child of ICT-based sexual abuse? What is the impact on a child of ICT-based sexual abuse? How do I stay secure on the Internet? Why is promoting safe use of ICT important? What does the school's Mobile Phone Policy Include?

6 Where can we learn more about Prevent? What do we have to do?

7 Do we have to have a separate *Prevent* Policy? What IT filtering systems must we have? What is the definition of a visiting speaker? Do we have to check all our visiting speakers? What checks must we run on visiting speakers? What do we have to record in our Single Central Register about visiting speakers?

8 What training must we have? What are the potential legal consequences if we do not take the *Prevent* duty seriously? What are the rules for publishing content online?

Use of video conferencing such as Zoom/Microsoft Teams video

OLA is using Zoom technology and Microsoft Teams Video as part of its remote learning technology. The following security guidance was issued by Zoom on 4 April. This guidance has been forwarded to all staff. This offers further practical guidance on how to generate a secure virtual meeting. Zoom has now enabled passwords on meetings and turned on Waiting Rooms by default as additional security enhancements to protect privacy. The waiting room is a virtual staging area that prevents people from joining a meeting until the host is ready.

OLA recognises that any enforced period of remote learning has the potential to be a time of great stress for parents, teachers and pupils. As a community we should play our part in helping families get used to remote learning. As this relates to pupils it means:

- No inappropriate, rude or continuous/unnecessary comment on zoom chat
- No silly behaviour and unkind comments
- No disruption of lessons

Where remote learning is imposed, pupils will be issued with guidelines about how to behave on zoom and online.

Every time pupils decide to behave immaturely online:

- *another pupil has learned less content*
- *a parent may have had to intervene, when they are in the middle of their own work*
- *you will have added stress to another family's routine and day*
- *you have disrupted the time the teacher has put aside, in the midst of their own family lives*

Zoom guidance for Lower school lessons:

- No animals or toys to be brought to Zoom lessons
- Children must be dressed in appropriate clothing/must be fully dressed when attending the Zoom lessons
- If possible, your child should sit in a quiet room with minimal background noise (preferably without the television on.) and away from siblings if possible.
- Children must only share their screens when asked to. Likewise, the chat facility must only be used with teacher permission.
- Changing backgrounds is not allowed. It is distracting and interferes with your own video picture. If you are on a laptop, using speaker view rather than gallery view is very helpful.
- The teacher will mute / unmute people. You can leave all the controls alone!
- No eating or drinking.
- Make sure your face can be seen properly.
- If you have to use a mobile device, prop it up against something and leave it still.
- Sit up properly at a table – no lying on beds!
- The teacher will start the call at the given time, not before. Don't go on too early!
- Behaviour should be of the same standard online as it is in the classroom. Take turns to speak. Put up your own hand or raise the virtual hand if you want to contribute. Anybody behaving inappropriately will have their video switched off temporarily and a reminder will be given about the rules. Have the books and equipment you need for the zoom session close to hand. Do not leave the meeting without permission of the teacher.

Zoom guidance for Senior school lessons:

- **Zoom should only be used when pupils are having a lesson using it** and should not be used by pupils for general communications at any other time. If they need to communicate with teachers they can do this over email, as normal. Teachers have found it useful to set up the chat for a class in zoom beforehand, as it makes it easier to start the call. Teachers also want to be able to use the chat function so that when they ask questions they can message in their answers, to make the sessions engaging and interactive. All year groups have been sensible and positive about this. However, *we have had an instance of inappropriate comments being used in the chat function by several pupils as zoom was set up for their class in advance of the lesson.* Pupils need to understand that Zoom is a classroom alternative and as such should only be used during lesson time. Use at other times, as a form of communication outside lessons, has cyberbullying implications and is not permitted. They have their own social media for communicating with each other, and teachers can check emails and respond to them that way. *We would be grateful if you could remind pupils of this.* In cases of misuse, staff and parents may be required to take screenshots straight away and email it in for the school to deal with.

- **We advise that the initiation of zoom comes from teachers rather than pupils.** However, it is at the discretion of the teacher whether they are comfortable to facilitate student's initiation of zoom meetings. *We have had an instance where a group of pupils were meeting via zoom and invited the teacher in, without the teacher being aware there was a zoom group meeting going on.* Whilst there is clearly a need for pupils to become familiar with the technology, there will be time for this to happen in the virtual classroom environment. There are clear boundaries in place to safeguard all parties and pupils are reminded that this is not a tool to be used for social gatherings.

- **Staff are aware that all zoom sessions must start by ASKING PUPILS if they are all happy to show their image in a video**. Any pupils that are not happy must switch the video function off. Most parents of pupils on the 'denied photo permissions' list have been contacted and have consented to waiving the denial for the purposes of remote learning only.

- **Pupils MUST behave appropriately** following the same behavioural principles as they would do in school. Instances of inappropriate behaviour must be sent to the Year Tutor, copying in BRey. This includes the inappropriate use of zoom technology itself.
    - The teacher is at liberty to ask a zoom invitee to leave the meeting if they are inappropriately dressed or their behaviour is not deemed appropriate.
    - A pupil can be asked to leave a meeting if their comments and contributions are of a silly nature or not appropriate to the lesson material. Pupils must learn to develop maturity in their use of zoom.

In relation to the use of zoom, it should also be noted that:

- Pupils will be invited to join a zoom meeting by their class teacher at appropriate points in a run of weekly lesson tasks according to when these lessons occur in the school timetable. This will either be through an e-mail invite or via a Firefly task.
- Pupils and staff must sign up to zoom using their school e-mail address
- Where 1:1 zoom meetings are required, such as for individual music lessons or learning support, zoom meetings may be recorded for safeguarding purposes. Individual music teachers will communicate directly with parents on how they will organise the lessons and also to agree on a system that is going to keep all parties safe.
- Where zoom meetings are recorded, a pupil is able to turn off their video link so that their image does not appear. This is important for those pupils with photo restrictions. Any parent who does not wish their son/daughter's image to appear on any recording, should advise the pupils to turn off the video function at their end. Teachers will also be asked to clarify this with pupils at the start of any zoom session.
- Any recordings from Zoom meetings will be stored in One Drive and then deleted at the end of the period of remote learning.
- We would advise that the initiation of zoom comes from teachers rather than pupils. However, it is at the discretion of the teacher whether they are comfortable to facilitate student's initiation of zoom meetings. During the last week of trials, this

has worked well for some teachers, with students zooming their teachers when they have needed advice. Pupils have valued this support.

- All pupils and staff must read the Responsible User Agreement for Remote Learning.
- We recognise that many pupils have personal computers in their bedrooms and this also provides a quiet space for them to work. In the circumstances of remote learning, we will allow pupils to join a zoom meeting from their bedroom, providing they are suitably dressed and are part of a group/class meeting. For safeguarding purposes, meetings may be recorded
- We are conscious of the potential for limited devices in families
- The potential for screen fatigue is a pastoral concern which will require monitoring. Zoom should be used as a tool to supplement learning, rather than being the primary teaching method. Pupils also need to have 'zoom-free' times when they can work independently.
- As stated previously, Zoom sessions can be recorded and the audio sent through to pupils afterwards if pupils are not able to join at the anticipated time. This can be made available to pupils via Firefly or shared from One Drive.

Online Behaviour

- All pupils should download the Zoom App using their school e-mail address
- When invited to be part of a zoom meeting, the teacher is in control of the meeting. A set of 'zoom' guidelines will be published. Any attempt to talk over/change the display/disrupt the lesson in any way will be noted and sanctioned upon return to school. We expect the highest standards of behaviour from pupils, as we would in class.
- Unless otherwise agreed by the teacher, under no circumstances should anyone other than the teacher attempt to begin a video or voice call. Inappropriate behaviour will be recorded and will result in sanctions once OLA reconvenes.
- If a pupil has restrictions on their photo being used in school, they should ensure they have the video function disabled when they join a zoom meeting.
- Where a zoom meeting involves 1:1 tuition (Music lessons, LS lessons), these zoom sessions will be recorded for safeguarding purposes.

Appendix 1 – Our Lady's Abingdon (OLA) Student and Parent acceptable use policy

The acceptable use policy below is expected to be read and signed by all students in Key Stage 3 and above. For our students in Key Stage 2, we do not ask these students to sign, however our staff will discuss and teach the core aspects of Online Safety including using technology respectfully, and we ask parents to have read and understood the policy to support us with keeping children safe when using devices.

All students must follow the rules outlined in this policy when using school ICT resources and equipment, including all Internet access and the Virtual Learning Environment (Teams and the student portal), accessed from both in and outside of school, and on school-provided or personal electronic devices. Breaking these conditions may lead to: confiscation of any electronic devices, close monitoring of the student's network activity, investigation of the student's past network activity, withdrawal of the student's access and, in some cases, permanent removal from the School and even criminal prosecution. Students are also expected to take care of school-issued electronic devices and any damage to them may result in charges to replace or fix damaged devices. Misuse of the Internet will be dealt with in accordance with OLA's *Positive Behaviour Code* and, where there is a safeguarding risk, the *Safeguarding & Child Protection Policy*. The school is not responsible for any loss of data on the network, computers connected to the network or data storage used on the network (including USB memory sticks). Data held on the network will be backed up for a limited period. Students are responsible for backups of any other data held. Use of any information obtained via the network is at the student's own risk.

Acceptable Use Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc.)
- If I arrange to meet people off-line who I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not use the school systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school.

- I will only use my own personal devices (mobile phones/USB devices etc.) in school if I have permission. I understand that, if

I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include loss of access to the school network/internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Student agreement:

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I use my own devices in the school (when allowed) e.g. mobile phones, USB devices etc.
- I use my own equipment out of the school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, website etc.

Print student name………………………………………………………………………… Class …………………………

Student Signature………………………………………………………………………….Date……………………………

Parent/Guardian agreement:

I understand that my child has agreed to accept the terms of the Online Safety and Student AUP Policy and I confirm that I accept the terms of the agreement. If my child brings any personal electronic devices to school, I understand that the student is responsible for its safekeeping and appropriate usage while in transit to and from and on campus.

I have read and understood the Online Safety policy and agree to check any updates, which are made available on the Parent Portal.

Print Parent/Guardian name…………………………………………………………………………………………………..

Parent/Guardian Signature……………………………………………………………… Date…………………………….

Appendix 2: Our Lady's Abingdon (OLA) Student Acceptable Use Policy – for younger pupils (KS2)

This document sits alongside OLA's E-SAFETY AND ICT ACCEPTABLE USE POLICY

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of computers/tablets and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer/tablet

Signed (child): --

For Parents:

I understand that OLA has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that OLA will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that OLA cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's/daughter's activity on the systems will be monitored and that OLA will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform OLA if I have concerns over my child's online safety.

Signed (parent): --

Appendix 3 – Our Lady's Abingdon (OLA) Staff and Volunteer Acceptable Use of ICT Policy:

To ensure that members of staff and volunteers are fully aware of their professional responsibilities when using information systems and when communicating with students, they are asked to sign this Acceptable Use Policy. Members of staff should consult the school's Online Safety policy and Staff Code of Conduct for further information and clarification. You must not use any ICT on-site until you have signed this AUP document and logged it with HR.

- I will respect all ICT equipment/facilities at OLA and will report any faults I find or any damage I accidentally cause.
- I agree to abide by this policy in respect of any of my own ICT equipment or mobile devices that I bring on site. If any ICT device (personal or school-issued) is being used inappropriately or illegally on site (or inappropriately in the presence of students), the Head may request that the device be monitored. Failure to comply with the monitoring could result in informing the appropriate authorities.
- I understand that no photographs of students may be taken with or stored on my personal electronic devices, including cameras, iPads, mobile phones, or personal computers.
- Photos of students should not be uploaded to personal social media accounts
- I am familiar with the OLA's *Data Protection Policy* and I agree I am responsible for the security of all personal data in my possession. I agree that all personal data that relates to an identifiable person and is stored or carried by me on a removable memory device will be encrypted or contained within password-protected files to prevent unauthorised access.
- I am responsible for my use of my own log-in details and if I suspect that my log-in details have become known to others then I will immediately ask for these details to be changed.
- I agree that my use of OLA's ICT equipment/facilities will be monitored and may be recorded at all times. I understand that the results of such monitoring and recording may be shared with other parties if I break the terms of this Acceptable Use Policy.
- I will not deliberately attempt to access any unsuitable websites, services, files or other resources when on-site or using OLA's equipment/facilities. I understand that I may temporarily access-blocked websites, services and other online resources using only tools that are provided by OLA. I agree that I will not display blocked websites, services and other resources to others until I have fully assessed the materials and have found them to be entirely suitable for the intended audience.
- I agree that the provision of OLA ICT equipment/facilities including the email and Internet system are for educational purposes, although limited personal use is permitted provided that this is not done during normal working time and does not contravene any of the other clauses in this document.
- I am aware that downloading copyright materials, including music and video files without paying the appropriate licence fee is often a criminal act. I am aware that any involvement in criminal acts relating to the use of ICT on-site or using OLA equipment/facilities may result in disciplinary or legal action. I will not deliberately engage in these acts.
- I will not deliberately view, send, upload or download any material that is unsuitable for the school environment whilst I am in that environment or using any ICT equipment/facilities belonging to OLA. If I accidentally encounter any such material then I will immediately close, but not delete in the case of emails, the material and immediately report it to the Online Safety Officer or to a senior member of staff. I will not be penalised if I view unsuitable material accidentally and by reporting such incidents I will help to improve Online Safety. If I am in any doubt about the suitability of any material, or if a colleague raises any doubts, then I will not (re)access the material without the agreement of the Online Safety Officer. I will not access any material that the Online Safety Officer has rated as unsuitable.
- Unless specifically authorised to do so, I will not disclose any of my personal details, other than those that identify me professionally, nor log any such details on websites whilst using OLA equipment or facilities. If I disclose any additional personal details contrary to this instruction, then I agree that these details can be recorded and that I will not hold OLA responsible for maintaining the security of the details I have disclosed.
- I agree that professional standards of communication will be maintained at all times. I recognise that staff should not communicate with students through personal electronic devices or methods such as social networking sites, blogging, chat rooms, text messaging, messenger applications or private email. Instead, only the school email system may be used.

Print Name ______________________ Signed _________________________ Date:_________________

Appendix 4 - Mobile and Smart Technology Policy, including taking and storing images of students

Legal Status:
Teaching Online Safety in School: DfE 2019
Cyberbullying: Advice of Headteachers and School Staff: DfE, 2014
Department for Education's published guidance on the use of mobile phones and UK law governing the use of mobile phones while driving.

Applies to: This policy applies to all individuals who are to have access to and or be users of personal and/ or work-related mobile phones within the broadest context of the setting environment. This will include our students, parents and carers, volunteers, visitors, contractors and community users. This list is not to be considered exhaustive.

Related documents:

- Safeguarding & Child Protection Policy
- Positive Behaviour Code
- Anti-Bullying Policy

Availability:
This policy is made available to parents, staff and students in the following ways: via the School website, parent portal and on request, a copy may be obtained from the Office.

Monitoring and Review: This document will be subject to continuous monitoring, refinement and audit by the Head. This document was reviewed and agreed by the Governing Board in September 2022 and if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require, prior to September 2023, the policy will be reviewed accordingly.

Signed:

Reviewed: September 2022
Next Review: September 2023

Head	DSL	Chair of Governors
Mr Daniel Gibbons	Chrissi Sharkey	Freddy El Turk
Signed: Daniel Gibbons	Signed: CSharkey	Signed:

Introduction: Whilst we welcome the use of mobile phones and cameras for educational purposes and the convenience they offer and recognise that learning to use digital technology is an important part of the ICT and wider curriculum, equally we have to ensure the safeguarding needs of the students are met and staff, parents and volunteers are not distracted from their care of students. Mobile phones, alongside other technologies aim to change the way we communicate. This speed of communication will often provide security and reassurance; however, as with any other form of technology there are associated risks. Students and young people must be encouraged to understand such risks, to enable them to develop the appropriate strategies which will keep them safe. Acceptable use and management of mobile phones is therefore to be agreed by all service users. There is to be a clear expectation that the personal use of mobile phones is to be limited to specific times and uses set out within the policy.

Aims: The aim of this Policy is to protect all users from harm, by ensuring the appropriate management and use of mobile phones by all individuals who work or visit our school, including students themselves. Students and young people are also to be empowered with the skills to manage the changes in technology in a safe and appropriate way; and to be alert to the potential risks of such use. This is to be achieved through balancing protection and potential misuse. It is therefore to be recognised that alongside the potential risks, mobile phones continue to be effective communication tools. This in turn is to contribute to safeguarding practice and protection.

Policy statement: It is to be recognised that it is the enhanced functions of many mobile devices that will give the most cause for concern; and which should be considered the most susceptible to potential misuse. Examples of misuse are to include the taking and distribution of indecent images, exploitation and cyberbullying. It must be understood that should mobile phones be misused, there will be a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to students and young people, so the needs and vulnerabilities of all must be respected and protected.

Mobile phones will also cause an unnecessary distraction during the working day and are often to be considered intrusive when used in the company of others. It will often be very difficult to detect when mobile phones are present or being used. The use of all mobile phones needs to be effectively managed to ensure the potential for misuse is to be minimised.

Code of conduct: A code of conduct is promoted with the aim of creating an informed workforce, who will work together to safeguard and promote positive outcomes for the students and young people in their care. It is to be ensured that all teachers and staff will:

- Be aware of the need to protect students from harm.
- Have a clear understanding of what constitutes misuse.
- Know how to minimise risk.
- Be vigilant and alert to potential warning signs of misuse.
- Avoid putting themselves into compromising situations which could be misinterpreted and lead to potential allegations.
- Understand the need for professional boundaries and clear guidance regarding acceptable use.
- Be responsible for the self-moderation of their own behaviours.
- Be aware of the importance of reporting concerns immediately.

Guidance on Use of Mobile Phones by Teaching Staff: The following points apply to all staff and volunteers at our school and apply to the use of all mobile devices to ensure the quality of supervision and care of the students, as well as the safeguarding of students, staff, parents and volunteers in the school.

OLA allows staff to bring in mobile phones for their own personal use. However, they must be kept away in closed drawers or their bags when teaching, and are not allowed to be used in the presence of students. They may be used during working hours in a designated break away from the students. Staff are not permitted to use recording equipment on their personal devices to take photos or videos of students. If staff fail to follow this guidance, disciplinary action will be taken in accordance to OLA Disciplinary Policy. During outings, nominated staff will be permitted to have access to their own mobile phones, which are to be used for emergency contact only. During off-campus activities, i.e. field trips and overnight excursions, trip leaders will be provided with a school-issued mobile phone in good working condition. School-issued mobile phones must be switched on and turned to loud to ensure that staff can be contacted by the school. Contact numbers for all members of staff accompanying the students must be left at Reception and a list of contact telephone numbers for all students should be with the leader of the off-site activity (although these must be kept confidential).

If staff need to make an emergency call, (such as summoning medical help or reporting an intruder on the premises) they must do so irrespective of where they are, via their own mobile phone or a school phone. Staff should provide the school number to members of the family and next of kin so in an emergency the member of staff can be contacted on the school phone. Staff must ensure that there is no inappropriate or illegal content on their phones or mobile devices. Should any member of staff become aware of inappropriate use of a mobile phone, this should be reported to a member of the LT, and may be subject to disciplinary action.

All teachers are responsible for the storage of school mobile devices, which should be locked away securely when not in use. Images taken and stored on school devices should be uploaded to the school's secure network and deleted from the device when no longer required. Staff are not to use their own equipment to take photos of students. Under no circumstances must devices of any kind be taken into the student toilets (this includes any device with photographic or video capabilities).

Guidance on staff use of social media: Staff must not post anything onto social networking sites such as Facebook that could be construed to have any impact on the School's reputation. (We advise all our staff to carefully restrict their Facebook profiles to ensure they cannot be contacted by parents and students; this could involve removing their last name from their page). We explain to staff that although they are able to accept friendship requests from friends, who may also be parents of students at the school, staff must be aware of the potential issues this could cause. Staff must not post anything onto social networking sites that would offend any other member of staff or parent. If any of the above points are found to have occurred, then the member of staff involved will face disciplinary action, which could result in dismissal. Where email contact is initiated by students who have left Our Lady's Abingdon, employees may reply from a school email address only with blind copies to line managers **and** the DSL. Staff must not accept friendship requests from students on roll and we advise staff not to accept requests from former students.

Guidance on Use of Mobile Devices by Students (3G, 4G and 5G access): Dependent on age, some students are permitted to have mobile devices whilst on the school grounds. However, the school recognises that by using devices which have access to 3G, 4G and 5G mobile phone networks, this can result in children having unlimited and unrestricted access to the internet, which could lead to some children, whilst at school or college, sexually harassing their peers via their mobile and smart technology, sharing indecent images: consensually and non-consensually (often via large chat groups), and viewing and sharing pornography and other harmful content. The school takes precautions to ensure that students limit access to their personal mobile devices during the school day, and reserves the right to confiscate and monitor personal devices when deemed necessary for safeguarding concerns. For students in KS2, mobile phones should be turned off and be lodged with the school office. For students in KS3/KS4, mobile devices should be switched off and kept securely in lockers or in their school bag unless permission has been given by the classroom teacher, such as for use in note taking or data collection. In the event of a mobile phone being used in a lesson without permission from the teacher, the phone should be confiscated and given to the Head of Section.

The School has the right to confiscate and search any mobile electronic device (personal or school-issued) if it suspects that a student or staff member is in danger or has misused a device. This will be done in accordance with the School's policy on searching and confiscation as set out in the Positive Behaviour Code.

Unacceptable Uses: In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, use the internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in the OLA Dining Hall.

- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment.
- Using mobile devices to intimidate, bully, harass, threaten, attempt to radicalise others or breach copyright laws is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to our Anti-bullying Policy)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to the school.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinary consequences.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- Safeguarding, privacy and respect are paramount at OLA. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and may be requested to turn over the device to the Head and/or the Designated Safeguarding Lead.
- For safety reasons, headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in OLA dining hall.
- Students are reminded that 'sexting' (sending or posting images or videos of a sexual or indecent nature) is strictly prohibited by the school and may constitute a criminal offence. Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. OLA will treat incidences of sexting (both sending and receiving) as a safeguarding issue and students concerned about images that they have received, sent or forwarded should speak to any member of staff for advice.

This may result in disconnection from the school network, confiscation of the mobile technology and/or legal or civil disciplinary action. Uploading images and sound is only permissible if the subject involved gives permission and if in doing so, School and statutory guidelines are not breached.

Theft or damage: Mobile phones or any mobile devices that are found in the school and whose owner cannot be located should be handed to the front office reception. The school accepts no responsibility for replacing lost, stolen or damaged devices. The school accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school. **It is strongly advised that students use passwords/pin numbers to ensure that unauthorised phone calls cannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.**

Inappropriate conduct: Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.

Use of images: displays etc

We will only use images of our students for the following purposes:

- Internal displays (including clips of moving images and yearbooks) on digital and conventional notice boards within OLA premises.
- Communications with OLA community (parents, students, staff), for example newsletters and E-learning Journals.
- Marketing OLA, both digitally by website, by prospectus, by displays at educational fairs and other marketing functions [both inside the UK and overseas] and by other means.

Storage and Review of Images: Images of students should be stored securely on the school network. Digital photographs and videos are reviewed annually and are deleted when no longer required. We regularly check and update our web site, with expired material deleted.

OLA Website and Social Media Pages: Photographs and videos may only be uploaded to the school’s website or social media accounts with the Head’s approval. Student’s surnames are never used on our website or social media pages.

Images that we use in displays and on our web site: The images that we use for displays and communications purposes never identify an individual student. Instead, they name the event, the term and year that the photograph was taken (for example, ‘Sports Day, Summer Term 2019’). We only use images of school activities, such as plays, concerts, sporting fixtures, prize-giving, school trips etc. in their proper context. We never use any image that might embarrass or humiliate a student. Students are always properly supervised when professional photographers visit OLA. Parents are given the opportunity to purchase copies of these photographs.

External Photographers: Professional photographs are taken throughout the year at school shows, by local media and Professional School Portraits. The Head ensures that professional photographers are DBS checked and that they have their own stringent regulations, which ensure safeguarding of students from inappropriate use of images.

Media coverage: We will always aim to notify parents in advance when we expect the press to attend an event in which our students are participating, and will make every effort to ensure that images including students whose parents or guardians have refused permission for such images of their students to be used are not used. We will always complain to the Press Complaints Council (PCC) if the media fails to follow the appropriate code of practice for the protection of young people, including the students of celebrities.

Staff induction: All new teaching and office staff are given guidance on the school’s policy on taking, using and storing images of students.

Parents/Visitors and Volunteers use of mobile phones/cameras within the school buildings (Including Photographing Pupils: Parents must ensure mobile phones/cameras are not on display (switched off or silent mode) while in the presence of students or in public areas of the school such as during meetings and school events. If staff observe that parents are using their mobile phones whilst in school, we will politely remind visitors as to why we do not permit the use of mobile phones in and around the school. The exception to this would be at an organised event. Staff should remind parents regularly of school policy with regard to mobile phone use with the following statement on weekly emails, when announcing events: "You are welcome to photograph your child at this event providing the images are for personal use only (e.g. a family album) and so are exempt from data protection Laws. Please be aware these images (which may include other students) must not be shared on social networking sites or other web-based forums since we regard this as 'making the image public'. Sharing images, or uploading them into a 'public space', is likely to be in breach of data protection." If they wish to make or take an emergency call, they may use the office and the school phone. OLA records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

Parents are welcome to take photographs of their own students taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others. Flash photography can disturb others in the audience, or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events. Parents are also reminded that copyright issues may prevent us from permitting the filming or recording of some plays and concerts. We always print a reminder in the programme of events where issues of copyright apply. Additionally, the school records images of students, both through moving pictures and stills, for assessment and reporting of progress, as well as celebration of their activities. It goes to some lengths to photograph professionally events and performances, which are available on request (or through purchasing), particularly in order to avoid distraction of students while performing and disturbance within the audience.

When students join OLA, we ask parents to sign consent for photographs and videos to be taken for such purposes. If consent is withheld, this must be made clear when the consent form is returned to school so that photographs/videos are not published of the individual child concerned. The students take part in various events throughout the year, such as assemblies, sporting events, drama and musical productions, field trips, the international festival, etc. Parents are welcome to take photographs of these memorable events, which may include groups of students. If a child takes part in the events, the parents are consenting to their child possibly being photographed or included in a group photograph by other parents. Wherever possible, parents who take photographs of groups of children who are in the care of the school should gain consent first, ensuring that once any photographs are taken, they are stored safely and not posted to social media. The school recognises that it cannot police parents taking photographs of pupils who are outside school grounds and not in the school's care, however posting such pictures online may be in breach of data protection laws without consent of all people within the photograph.

Other mobile technology: At OLA, we recognise the value of mobile technology within our curriculum and our students' accommodation. Within the Senior school, students are required to bring their own devices to support their studies. Any personal device that students bring to the school must be used appropriately in line with the Students' Acceptable Use Policy and must be kept securely. Where a student is found to be misusing a school or personal device, or accessing inappropriate content, the device may be confiscated by the school and appropriate action taken. When accessing the school WiFi, staff and students must adhere to their ICT Acceptable Use Policy. Staff, students, volunteers and parents are responsible for their own mobile devices and the school is not responsible for theft, loss, or damage.

Driving and the law: The use of hand-held phones while driving, whether to make or receive a call, is prohibited. The only exception to this will be in the event of a genuine emergency call to 999 or 112, if it would be unsafe for the driver to stop. Hand-held mobile phones used with an earphone and microphone are covered under the ban, as they still require the user to hold the phone to press buttons or to read a message on the phone's screen. Mobile phones must instead be directed to the message/voicemail service while driving. The Head will not assist in the payment of any fine levied against anyone using a hand-held mobile phone while driving. An employee will be regarded as driving if the engine is running, even if the vehicle is stationery. Notification of any contravention of these requirements may be regarded as a disciplinary matter.

Appendix 5 – Our Lady's Abingdon (OLA) Use of photographs of students and data protection (completed by all new parents)
The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use OLA digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons. Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name/initials will be used. OLA will comply with the Data Protection Act and request parent's/carers permission before taking images of members of OLA. We will also ensure that when images are published that the young people cannot be identified by the use of their names. In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Photographs
Our Lady's Abingdon would like your permission to use photographs of your child for marketing and publicity purposes including our website, prospectus, adverts, press releases and other marketing literature such as brochures and leaflets. We will not use names next to photographs of students on the website (in accordance with the DfE guidelines).

Parent/Guardian's name: ____

Pupil's name: ____

Pupil's year group/form: ____

Please circle the appropriate response.

As the parent/carer of the above student/pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
• to support learning activities.	Yes/No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes/No

Signed: --

Date: --

Data Protection Statement
Information about parents/carers is collated, stored and used by Our Lady's Abingdon for the purposes of keeping you informed of events and activities concerning Our Lady's Abingdon and for fundraising. By signing this form, you consent to Our Lady's Abingdon using your data in this way. This information will not be used for any other purpose or passed to any person outside the school without your consent.

I consent to Our Lady's Abingdon using my data for the stated purposes □

I do not consent to Our Lady's Abingdon using my data for the stated purposes □

Signature: _______________ Date: ____

Appendix 6: Online Safety FAQs

How will the policy be introduced to Students?

- Rules for Internet access will be posted in all rooms where computers are used
- Students will be informed that Internet use will be monitored
- Instruction in responsible and safe use should precede Internet access
- A module on responsible Internet use will be included in the PSHE programme covering both home and school use.
- Students will be informed that network and Internet use will be monitored and appropriately followed up.
- Students will be made aware of the acceptable use of technology and sign upon enrolment

How will ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Use of portable media such as USB sticks, SD Cards and Hard Drives to carry work should be kept confidential by staff and not used in public computers.
- Files held on the school network will be regularly checked
- All network system and administration passwords are to be recorded by the IT Department and kept in a secure place with regular updates

How will staff be consulted and made aware of this policy?

- All staff must accept the terms of the 'Responsible Internet Use' statement included in the staff handbook before using any Internet resource in school.
- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff including teachers, learning support assistants and support staff will be provided with the School Online Safety policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible Internet use, and on the school Internet policy will be provided as required.
- Breaching this Online Safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.
- Staff will read the ICT Acceptable Use Policy and sign the form prior to using school ICT equipment in the school

How will complaints regarding Internet use be handled?

- Responsibility for handling complaints that have progressed to Stage 2 will be delegated to a relevant member of the Senior Leadership Team.
- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with our Safeguarding & Child Protection Policy and procedures.
- Students and parents will be informed of the complaint procedure which is available on the Our Lady's Abingdon website.
- Parents and Students will need to work in partnership with staff to resolve issues.
- There may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

How will parents' support be enlisted?

- Parents' attention will be drawn to the responsible Internet use policy in newsletters, the parent portal and on the school website.
- Internet issues will be handled sensitively to inform parents without undue alarm.

- A partnership approach will be encouraged with parents and could include information booklets, practical sessions and suggestions for safe Internet use at home.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.
- We will maintain a list of Online Safety resources for parents.
- Parents will be invited to attend an Online Safety workshop annually.

Why is the use of Internet and ICT important?

Not only is familiarity with the use of ICT equipment a core requirement, but the efficient use of the equipment and available resources is also considered key – for example, the use of email for efficient communication and the correct use of the Internet for research. Staff across the school are making increased use of ICT, which benefits not only the quality of teaching and support services but also their professional development. It is equally important that staff are properly equipped and supported to make the most efficient use of ICT resources. In particular, ICT is extremely beneficial in engaging our students, who have learning and physical disabilities. It can also help them to access parts of the curriculum, which they might not otherwise be able to engage with.

All students deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. Internet use is a part of the statutory curriculum and a necessary tool for staff and Students. The school has a duty to provide Students with quality Internet access as part of their learning experience. In order for the school to maintain such an environment for learners (students and adults) everybody must be aware of the need to ensure online protection (Online Safety) and subsequently understand the principles of this policy and the expectations of school practice as documented below.

How is the Safe Use of ICT and the Internet Promoted?

Our Lady's Abingdon takes very seriously the importance of teaching students (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community. Our Lady's Abingdon has in place an Internet firewall, Internet content filtering and antivirus software, and various IT security policies, which help to ameliorate the risk of accessing inappropriate and unauthorised material. However, no system is 100% safe and Our Lady's Abingdon will further promote safe use of ICT and the Internet by educating students and staff about the risks and the ways they can be mitigated by acting sensibly and responsibly. The school will ensure that the use of Internet derived materials by staff and Students complies with copyright law. Our Lady's Abingdon will help students to understand the risks posed by adults or young people, who use the Internet and social media to bully, groom, abuse or radicalise other people, especially students, young people and vulnerable adults. Internet safety is integral to the school's ICT curriculum and is also be embedded in our PSHEE and SMSC provision. The latest resources promoted by the DfE can be found at:

- The UK Safer Internet Centre (www.saferinternet.org.uk)
- CEOP's Thinkuknow website (www.thinkuknow.co.uk)
- PSHE Association (https://www.pshe-association.org.uk/)
- Google Legends (KS2) (https://beinternetlegends.withgoogle.com/en_uk)

How does the Internet and use of ICT benefit education in our school?

- Students learn effective ways to use ICT and the Internet including safe and responsible use.
- Access to worldwide educational resources including museums and art galleries.
- Educational and cultural exchanges between Students worldwide.
- Access to experts in many fields for students and staff.
- Staff professional development through access to national developments, educational materials and good curriculum practice.
- Communication with support services, professional associations and colleagues.
- Improved access to technical support.
- Exchange of curriculum and administration data with LA and DfE
- Support of the wider curriculum through the use of word processing, spreadsheet and presentation tools, specialist applications, and the use of the Internet for research purposes.

How will Students learn to evaluate Internet content?

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, evaluation and retrieval.
- Students will be taught what Internet use is acceptable and what is not and given clear guidelines for Internet use.
- If staff or Students discover unsuitable sites, the URL (address) and content must be reported to the teacher, Online Safety Officer or IT Department.
- Staff and Students should ensure that their use of Internet derived materials complies with copyright law
- Students will be taught the SIFT Model to be critically aware of the materials they read and show how to validate information before accepting its accuracy.
- Students will be taught to acknowledge the source of information used and to respect copyright.

How is Filtering Managed?

Having Internet access enables students to explore thousands of global libraries, databases and bulletin boards. They are also able to exchange messages with other learners and teachers throughout the world. All unsuitable websites will be filtered and automatically blocked by our security systems and will not be made accessible to students. In addition, students' usage of our network will be continuously monitored and repeated attempts to access unsuitable sites will alert our IT Department. The IT Department will tailor the filtering to suit the individual needs of subjects and the school generally appropriate to the age of students. Although this filtering uses the latest security technology, parents/guardians will wish to be aware that some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at Our Lady's Abingdon we believe that the benefits to students having access to the Internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. However, as with any other area, parents and guardians of minors along with Our Lady's Abingdon share the responsibility for setting and conveying the standards that students should follow when accessing and using these media information sources at school and/or at home. During school time, teachers will guide students towards appropriate material on the Internet. Outside school, families bear the same responsibility for guidance as they exercise with other information, sources such as television, telephones, films and radio.

- The school will work in partnership with parents/guardians, the Local Authority (LA) and Department for Education (DfE) to ensure systems to protect students are reviewed and improved.
- If staff or students come across unsuitable on-line materials, they must report it to the DSL or Chair of Governors immediately.
- The school will take every step to ensure that appropriate filtering systems are in place to protect students from unsuitable material and the methods used will be reviewed regularly.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation (www.iwf.co.uk).

How are Emerging Technologies Managed?

ICT in the 21st Century has an all-encompassing role within the lives of students and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in school and, more importantly in many cases, used outside of school by students may include:

- The Internet
- E-mail
- Instant messaging / video messaging apps (WhatsApp / WeChat / iMessage)
- Social media sites (Facebook, Instagram, Twitter, TikTok)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Video broadcasting sites (Popular: http://www.youtube.com/ ,Twitch)
- Chat Rooms (Popular www.teenchat.com, Discord)
- Gaming Sites
- Music download sites (Popular Apple, Spotify,)
- Smart Phones (where all of the above can be accessed)

- Mobile technology (e.g. games consoles)

How to React to Misuse by Students and Young People
• **Step 1:** Should it be considered that a child or young person has deliberately misused ICT, a letter will be sent to the parent or carer outlining the issue. The child or young person may be temporarily suspended from a particular activity.
• **Step 2:** If there are to be further incidents of misuse, the child or young person will be suspended from using the Internet or other relevant technology for an increased period of time. The parent or carer will be invited to discuss the incident in more detail with a member of the Leadership Team and the most appropriate course of action will be agreed.
• **Step 3:** The sanctions for misuse can be escalated at any stage, should it be considered necessary. In the event that misuse is deemed to be of a serious nature, steps 1 and 2 can be omitted. Should a child or young person be considered to be at risk of significant harm, the Safeguarding & Child Protection Policy must also be applied. Allegations of serious misuse will be reported to the most appropriate agency, for example, the Police or Children's Social Care.

In the event that a child or young person should accidentally access inappropriate material, it must be reported to an adult immediately. Appropriate action is to be taken to hide or minimise the window. The computer will not be switched off nor will the page be closed, as it may be necessary to refer to the site during investigations to allow effective filters to be put in place to prevent further inadvertent access.

How is Printing Managed?
The use of the ICT printers may be monitored on an individual basis to encourage careful use of printing resources. As well as being a significant capital cost, the consumables (ink, laser printer toner and drums, and paper) associated with printing represent one of the most expensive ongoing costs associated with ICT. Whilst the school would not wish to discourage the proper use of printers, it is important to ensure that printing facilities are used efficiently and effectively. Students and staff are asked to take care not to waste printing resources, for example by using "Print Preview" to check work before sending it to the printer and by using colour print only when necessary.

What are the categories of Cyber-Bullying? Seven categories of cyber-bullying have been identified:

- **Text message bullying** involves sending unwelcome texts that are threatening or cause discomfort;
- **Picture/video-clip bullying via mobile phone cameras** is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people. 'Happy slapping' involves filming and sharing physical attacks;
- **Phone call bullying via mobile phone** uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- **Email bullying** uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them.
- **Online grooming, Chat room and Social Networking Site abuse** involves sending menacing or upsetting responses to students or young people, or posting inappropriate material in a public digital locale.
- **Bullying through instant messaging (IM)** is an Internet-based form of bullying where students and young people are sent unpleasant messages as they conduct real-time conversations online.
- **Bullying via websites** includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

General Housekeeping:
The ICT equipment used by the school represents a considerable financial investment. It makes sense to treat it well so that it will remain in good working order. In addition, the ICT resource is finite e.g. computers can run out of disk space; users should be encouraged to think about the amount of file storage they use and the need to keep it well organised. The school does not currently operate a quota system for disk space or mailboxes, but will consider doing so should the need arise.
The following will apply:

- Treat ICT equipment with respect and keep areas around ICT equipment clean and tidy.

- Normal school rules and consideration of others applies.
- Keep the amount of storage you use to a minimum. Clear out old and unused files regularly.

Student Rules when using school ICT: Due to the variety of resources throughout the school, including the use of portable digital equipment, the following rules are to be considered as appropriate to the location and the resource.

- Obtain permission to access school-issued ICT resources.
- Food and drink must not be consumed near any computer equipment anywhere in the school.
- Any person found defacing or wilfully damaging ICT equipment will be required to correct the damage caused or pay for replacement.
- Computer/device faults should be promptly reported to the ICT Co-ordinator. Please do not attempt to repair them yourself.
- Be aware of correct posture. Always ensure that your chair is at the optimum height for you and that you are sitting correctly at a workstation when possible.
- <u>At the end of a session using an computer station</u>:
- Log off/shut down according to instructions.
- Replace laptops/equipment as directed.
- Wind up and put away any headsets.

What has Research into Cyber Bullying Found?

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or Internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Most cyber-bullying is done by students in the same class or year group and although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

- Between a fifth and a quarter of students have been cyber-bullied at least once over the previous few months.
- Phone calls, text messages and email are the most common forms of cyber-bullying.
- There is more cyber-bullying outside school than in.
- Girls are more likely than boys to be involved in cyber-bullying in school, usually by phone.
- For boys, text messaging is the most usual form of cyber-bullying, followed by picture/video clip or website bullying.
- Picture/video clip and phone call bullying are perceived as the most harmful forms of cyber-bullying.
- Website and text bullying are equated in impact to other forms of bullying.
- Around a third of those being cyber-bullied tell no one about the bullying.

What is the impact on a child of ICT based sexual abuse?

The impact on a child of ICT based sexual abuse is similar to that for all sexually abused students. However, it has an additional dimension in that there is a visual record of the abuse. ICT based sexual abuse of a child constitutes significant harm through sexual and emotional abuse. Recognition and response is recognising a situation where a child is suffering, or is likely to suffer a degree of physical, sexual and/or emotional harm (through abuse or neglect) which is so harmful that there needs to be compulsory intervention by child protection agencies into the life of the child and their family.

Why is Promoting Safe Use of ICT Important?

Our Lady's Abingdon takes very seriously the importance of teaching students (and staff) to use ICT - and especially the Internet - in a safe and responsible manner. This will have a positive impact on not only the use of ICT in school, but also outside school in the wider community.

What does the school's Mobile Phone Policy Include?

- The commitment to keep the students safe.
- How we manage the use of mobile phones at Our Lady's Abingdon taking into consideration staff, students on placement, volunteers, other professionals, Proprietor, visitors and parents/carers.
- How we inform parents/carers, visitors and other professional of our procedures.

- What type of mobile phones will be used on educational visits and learning outside the classroom.
- The consequences of any breaches of this policy.
- Reference to other policies, such as Whistleblowing and Safeguarding Children-Child Protection Policies.

What are the rules for publishing content online?

- Staff or Student personal contact information will not be published on the school website. The only contact details given on our website will be the school address and telephone number.
- Student's full names will not be used anywhere on the school website or other on-line space.
- We may use photographs of students or their work when communicating with parents and the wider community, in newsletters and in the school prospectus.
- Photographs will be checked to ensure that they are suitable (photos of students in swimwear would be unsuitable).

Appendix 7 - Our Lady's Abingdon (OLA) Student Acceptable Use of Mobile Phones and 3G/4G/5G compatible devices

It is our intention to provide within this policy an environment in which children, parents, and staff are safe from images being recorded and inappropriately used, in turn eliminating the potential use to interfere with the dignity and privacy of all individuals and thus compromise the confidentiality of the children in our care.

Purpose & Rationale

- The widespread ownership of Mobile phones and 3G/4G/5G compatible devices (referred to throughout this document as mobile devices) among young people requires that OLA administrators, teachers, students, parents and carers take steps to ensure that these devices are used safely and responsibly at school. This *Acceptable Use Policy* is designed to ensure that potential issues involving mobile devices can be clearly identified and addressed, ensuring the benefits that they can provide can continue to be enjoyed by our students.
- The school has established the following *Acceptable Use Policy for mobile devices* that provides teachers, students, parents and carers guidelines and instructions for the appropriate use of these devices during the time students are under the care of OLA, inclusive of the academic day, on campus and all educational visits.
- Students, their parents or carers must read and understand the Acceptable Use Policy as a condition upon which permission is given to bring mobile devices to OLA.
- The school recognises that personal communication through mobile devices such as mobile technologies is an accepted part of everyday life, therefore such technologies are to be used responsibly and in accordance to the Acceptable Use Policy.
- OLA accepts that parents/carers give their children mobile phones to protect them from everyday risks involving personal security and safety. There is also increasing concern about commuting long distances to school. It is acknowledged that providing a child with a mobile phone gives parents reassurance that they can contact their child if they need to speak to them urgently.

Responsibility:

- It is the responsibility of students who bring mobile devices to OLA to follow the guidelines outlined in this document.
  The decision to provide any mobile devices to their children should be made by parents or carers. It is important that parents understand the capabilities of these devices and the potential uses or misuses of those capabilities. If needed, guidance to this information can be signposted by OLA.
- Parents/carers should be aware that if their child brings any device, including a mobile phone to OLA, the school does not accept responsibility for any loss, damage or costs.
- Parents/carers are reminded that in cases of emergency, OLA remains a vital and appropriate point of contact and can ensure your child is reached in a relevant and appropriate way. Parents/carers are requested that in cases of emergency they contact OLA first so we are aware of any potential issue and may make any necessary arrangements.

Acceptable Uses:

- Mobile phones should be switched off and kept out of sight during lessons in order to minimize disruption or distraction.
- Mobile phones should not be used in any manner or place that could be disruptive to the normal OLA routine.
- OLA recognises the importance of emerging technologies present in modern mobile devices e.g. phones, camera and video recording, internet access, MP3 and MP4 playback, blogging, etc. Teachers may wish to utilise these functions to aid teaching and learning and students may have the opportunity to use their mobile phones or mobile devices in the classroom. On these occasions students may use their mobile phones in the classroom when express permission has been given by the teacher. The use of personal mobile phones in one lesson for a specific purpose does not mean blanket usage is then acceptable.
- Headphones/earphones should only be used during private study or travelling to and from OLA with permission from the teacher.

Unacceptable Uses:

- In order to protect one's privacy and respect to others, unless express permission is granted, mobile phones, laptops and mobile devices should not be used to make calls, send messages, surf the internet, take photos or use any other application during school lessons, other educational activities such as assemblies, or in the Dining Hall.

- Mobile devices should not disrupt classroom lessons with ring tones, music or beeping. They should be turned off during lesson times in order to respect the learning environment. Using mobile phones to bully and threaten other students is unacceptable. Cyber bullying will not be tolerated. In some cases, it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence it is unacceptable regardless of whether 'consent' was given. (Please refer to the Anti-bullying and Online Safety Policies.)
- Mobile phones are not to be used in changing rooms or toilets or used in any situation that may cause embarrassment or discomfort to their fellow students, staff or visitors to OLA.
- Disruption to lessons caused by a mobile phone or any mobile device may lead to disciplinary consequences.
- Safeguarding, privacy and respect are paramount at OLA. To this end, it is prohibited to take a picture of or record a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images and may be requested to turn over the device to the Head and/or the Designated Safeguarding Lead.
- Headphones/earphones should not be used whilst moving around campus during the school day, whilst waiting for or during lessons and assemblies, or in the dining halls.

Theft or damage:

- Mobile phones or any mobile devices that are found in OLA and whose owner cannot be located should be handed to the front office reception.
- OLA accepts no responsibility for replacing lost, stolen or damaged devices.
- OLA accepts no responsibility for damage to or loss of mobile phones or mobile devices while travelling to and from school.
- It is strongly advised that students use passwords/pin numbers to ensure that unauthorized phone calls cannot be made on their phones or other mobile devices. Students must keep their password/pin numbers confidential.

Inappropriate conduct:

- Under exam regulations, mobile phones are prohibited from all examinations. Students MUST give phones to invigilators before entering the exam hall. Any student found in possession of a mobile phone during an examination will have that paper disqualified. Such an incident may result in all other exam papers being disqualified.
- Any student who uses vulgar, derogatory, or obscene language while using a mobile phone may face disciplinary action.
- Students with mobile phones may not engage in personal attacks, harass another person, or post private information about another person using messages, taking/sending photos or objectionable images, and phone calls. Students using mobile phones to bully other students will face disciplinary action. (It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. As such, OLA may consider it appropriate to involve the police).
- Students must ensure that files stored on their phones do not contain violent, degrading, racist or pornographic images. The transmission of such images is a criminal offence, and OLA is obliged to report any findings of this nature to the police and local authority.
- Similarly, 'sexting' – which is the sending of personal sexual imagery - is also a criminal offence, which obliges OLA to report to the police and local authority.

Measures: The following measures may be used in consultation and conjunction with the Anti-bullying , Child Protection and Safeguarding, E-Safety and IT Policies. The Online Safety Coordinator (DSL) must be consulted when inappropriate conduct requires a mobile phone to be confiscated and searched.

- Students who violate the rules set out in this document could face having their phones and/or mobile devices held by teachers, Heads of Section or Assistant Heads until the end of the class period or study session. If the device is being used inappropriately the student must give it to the supervising adult if requested.
- Violation of the rules set out in this document are subject to the disciplinary measures set out in the Positive Behaviour Code, which can be found on the policy section of the school's Website.

I have read and understand this policy:

Student signature: ___________________________ Parents: Informed via email communication

Appendix 8 - Our Lady's Abingdon (OLA) Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

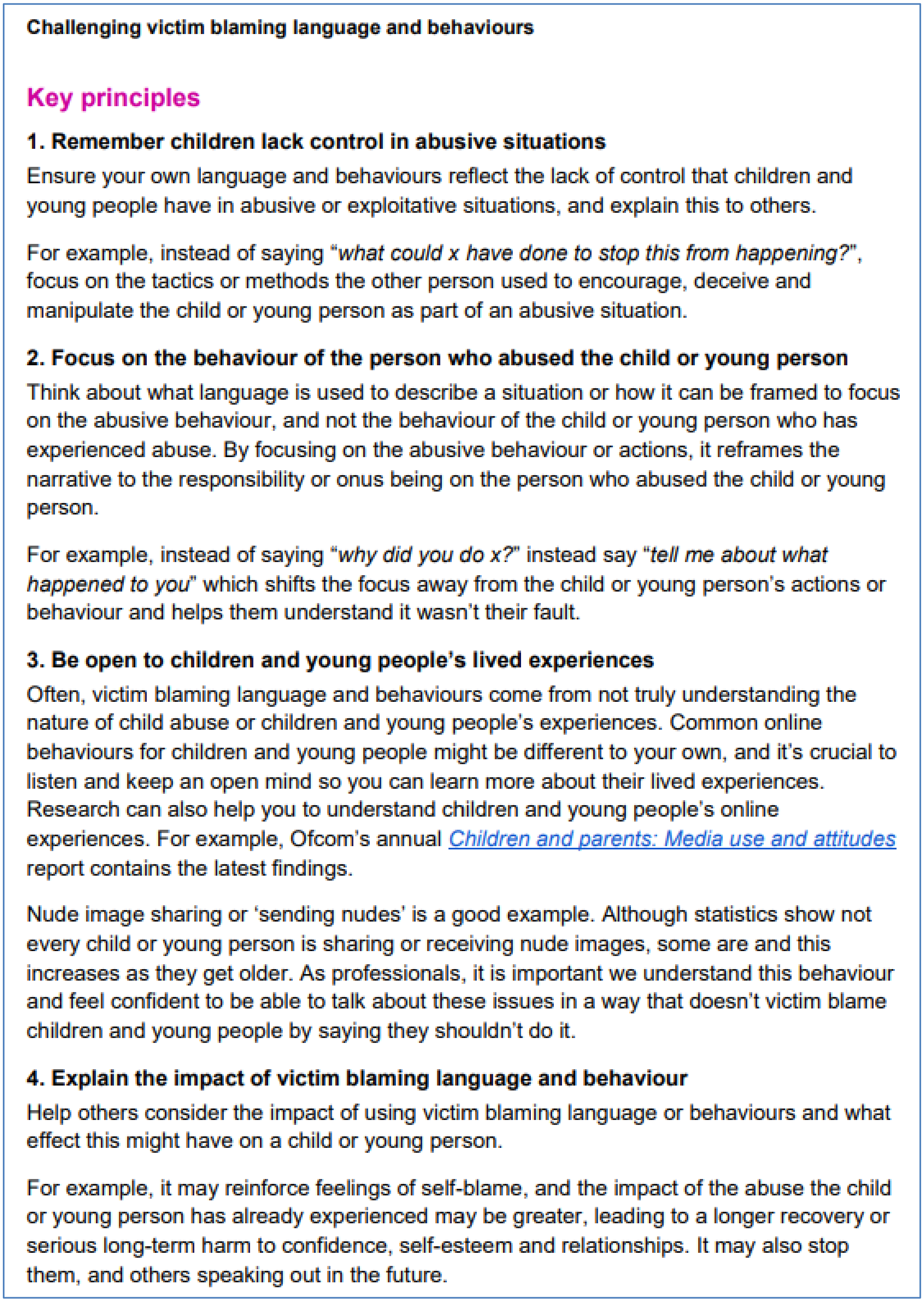
I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.
As the school is collecting personal data by issuing this form, it should inform community users about:

Name: .... Signed: .... Date:……………………………………….

Appendix 9: Challenging victim blaming language and behaviours



Challenging victim blaming language and behaviours

Key principles

1. Remember children lack control in abusive situations

Ensure your own language and behaviours reflect the lack of control that children and young people have in abusive or exploitative situations, and explain this to others.

For example, instead of saying "*what could x have done to stop this from happening?*", focus on the tactics or methods the other person used to encourage, deceive and manipulate the child or young person as part of an abusive situation.

2. Focus on the behaviour of the person who abused the child or young person

Think about what language is used to describe a situation or how it can be framed to focus on the abusive behaviour, and not the behaviour of the child or young person who has experienced abuse. By focusing on the abusive behaviour or actions, it reframes the narrative to the responsibility or onus being on the person who abused the child or young person.

For example, instead of saying "*why did you do x?*" instead say "*tell me about what happened to you*" which shifts the focus away from the child or young person's actions or behaviour and helps them understand it wasn't their fault.

3. Be open to children and young people's lived experiences

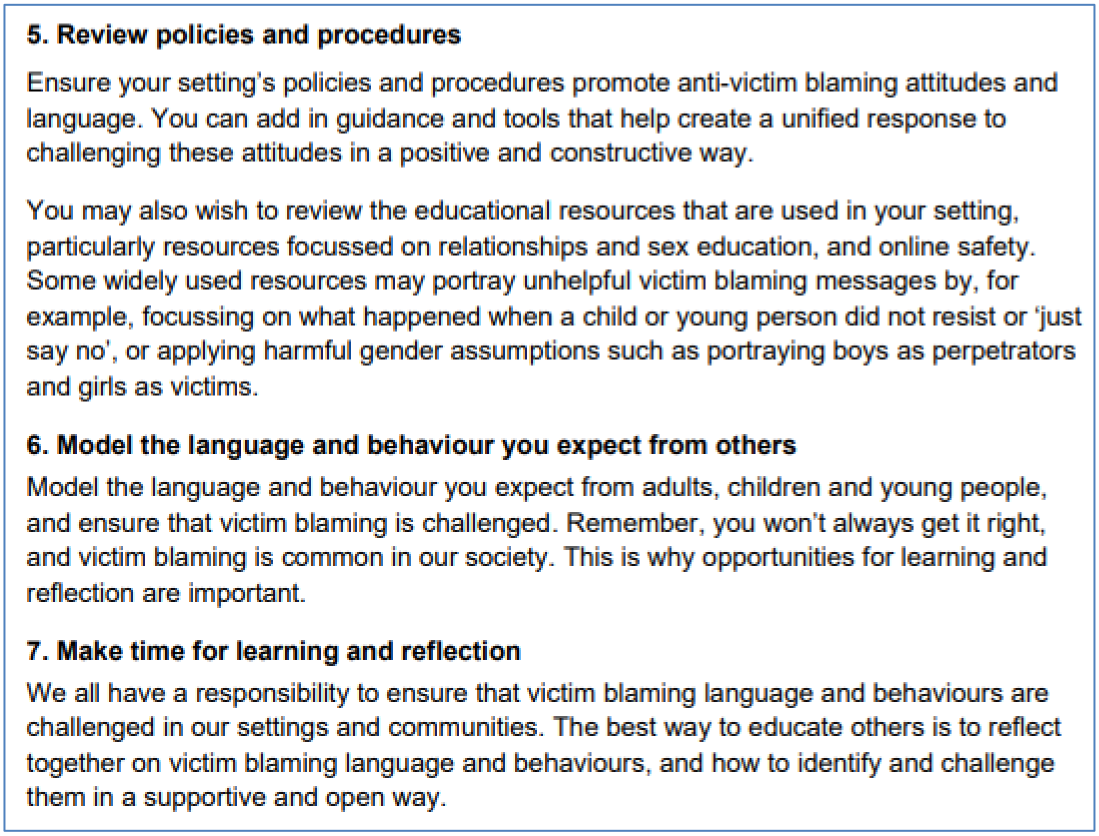
Often, victim blaming language and behaviours come from not truly understanding the nature of child abuse or children and young people's experiences. Common online behaviours for children and young people might be different to your own, and it's crucial to listen and keep an open mind so you can learn more about their lived experiences. Research can also help you to understand children and young people's online experiences. For example, Ofcom's annual *Children and parents: Media use and attitudes* report contains the latest findings.

Nude image sharing or 'sending nudes' is a good example. Although statistics show not every child or young person is sharing or receiving nude images, some are and this increases as they get older. As professionals, it is important we understand this behaviour and feel confident to be able to talk about these issues in a way that doesn't victim blame children and young people by saying they shouldn't do it.

4. Explain the impact of victim blaming language and behaviour

Help others consider the impact of using victim blaming language or behaviours and what effect this might have on a child or young person.

For example, it may reinforce feelings of self-blame, and the impact of the abuse the child or young person has already experienced may be greater, leading to a longer recovery or serious long-term harm to confidence, self-esteem and relationships. It may also stop them, and others speaking out in the future.



5. Review policies and procedures

Ensure your setting's policies and procedures promote anti-victim blaming attitudes and language. You can add in guidance and tools that help create a unified response to challenging these attitudes in a positive and constructive way.

You may also wish to review the educational resources that are used in your setting, particularly resources focussed on relationships and sex education, and online safety. Some widely used resources may portray unhelpful victim blaming messages by, for example, focussing on what happened when a child or young person did not resist or 'just say no', or applying harmful gender assumptions such as portraying boys as perpetrators and girls as victims.

6. Model the language and behaviour you expect from others

Model the language and behaviour you expect from adults, children and young people, and ensure that victim blaming is challenged. Remember, you won't always get it right, and victim blaming is common in our society. This is why opportunities for learning and reflection are important.

7. Make time for learning and reflection

We all have a responsibility to ensure that victim blaming language and behaviours are challenged in our settings and communities. The best way to educate others is to reflect together on victim blaming language and behaviours, and how to identify and challenge them in a supportive and open way.

Appendix 10: Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – https://www.saferinternet.org.uk/
South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/
Childnet – http://www.childnet-int.org/
Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline
Revenge Porn Helpline - https://revengepornhelpline.org.uk/
Internet Watch Foundation - https://www.iwf.org.uk/
Report Harmful Content - https://reportharmfulcontent.com/

CEOP

CEOP - http://ceop.police.uk/
ThinkUKnow - https://www.thinkuknow.co.uk/

Others

LGfL – Online Safety Resources
Kent – Online Safety Resources page
INSAFE/Better Internet for Kids - https://www.betterinternetforkids.eu/
UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety
Netsmartz - http://www.netsmartz.org/

Tools for Schools

Online Safety BOOST – https://boost.swgfl.org.uk/
360 Degree Safe – Online Safety self-review tool – https://360safe.org.uk/
360Data – online data protection self-review tool: www.360data.org.uk
SWGfL Test filtering - http://testfiltering.com/
UKCIS Digital Resilience Framework - https://www.gov.uk/government/publications/digital-resilience-framework

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - http://enable.eun.org/
SELMA – Hacking Hate - https://selma.swgfl.co.uk
Scottish Anti-Bullying Service, Respectme - http://www.respectme.org.uk/
Scottish Government - Better relationships, better learning, better behaviour - http://www.scotland.gov.uk/Publications/2013/03/7388
DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf
Childnet – Cyberbullying guidance and practical PSHE toolkit: http://www.childnet.com/our-projects/cyberbullying-guidance-and-practical-toolkit
Childnet – Project deSHAME – Online Sexual Harrassment
UKSIC – Sexting Resources
Anti-Bullying Network – http://www.antibullying.net/cyberbullying1.htm
Ditch the Label – Online Bullying Charity
Diana Award – Anti-Bullying Campaign

Social Networking

Digizen – Social Networking
UKSIC - Safety Features on Social Networks
Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media

Curriculum

SWGfL Evolve - https://projectevolve.co.uk
UKCCIS – Education for a connected world framework
Teach Today – www.teachtoday.eu/
Insafe - Education Resources

Data Protection

360data - free questionnaire and data protection self review tool
ICO Guides for Education (wide range of sector specific guides)

DfE advice on Cloud software services and the Data Protection Act
IRMS - Records Management Toolkit for Schools
NHS - Caldicott Principles (information that must be released)
ICO Guidance on taking photos in schools
Dotkumo - Best practice guide to using photos

Professional Standards/Staff Training
DfE – Keeping Children Safe in Education
DfE - Safer Working Practice for Adults who Work with Children and Young People
Childnet – School Pack for Online Safety Awareness
UK Safer Internet Centre Professionals Online Safety Helpline

Infrastructure/Technical Support
UKSIC – Appropriate Filtering and Monitoring
SWGfL Safety & Security Resources
Somerset - Questions for Technical Support
NCA – Guide to the Computer Misuse Act
NEN – Advice and Guidance Notes

Working with parents and carers
Online Safety BOOST Presentations - parent's presentation
Vodafone Digital Parents Magazine
Childnet Webpages for Parents & Carers
Get Safe Online - resources for parents
Teach Today - resources for parents workshops/education
Internet Matters

Prevent
Prevent Duty Guidance
Prevent for schools – teaching resources
NCA – Cyber Prevent
Childnet – Trust Me

Research
Ofcom –Media Literacy Research

Further links can be found at the end of the UKCIS Education for a Connected World Framework