OLA Safeguarding & Online Safety

(with reference to remote learning)

Appendix

Contents

0

Contents 1

Development/Monitoring/Review of this Policy 2

Roles and Responsibilities 3

Policy Statements 7

Communications (when working from site and remotely) 13

Dealing with unsuitable/inappropriate activities 21

Responding to incidents of misuse 23

Illegal Incidents 23

Other Incidents 25

School actions & sanctions 25

Student/Pupil Acceptable Use Agreement Template – for older students/pupils 29

Student/Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1/KS2) 32

Parent/Carer Acceptable Use Agreement Template 33

Staff (and Volunteer) Acceptable Use Policy Agreement Template 37

Acceptable Use Agreement for Community Users Template 40

Responding to incidents of misuse – flow chart 41

Record of reviewing devices/internet sites (responding to incidents of misuse) 42

Reporting Log 43

Training Needs Audit Log 44

Glossary of Terms 47

Development/Monitoring/Review of this Policy

This Safeguarding and online safety appendix has been developed by the **Whole School Safeguarding Team (WSST)** made up of:

- Principal
- Deputy Head
- DSL - Assistant Head (Safeguarding) and DDSL - Assistant Head (Pastoral)
- DDSL – Head of Lower School and DSL (EYFS)

It is overseen by the Chief Operating Officer and has been influenced by feedback from both staff and parents

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	
The implementation of this online safety policy will be monitored by:	*WSST*
Monitoring will take place at regular intervals:	*September 2020*
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:	*September 2020*
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 2020*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*OCC Safeguarding Officer, LADO, Police Liaison Officer*

The school 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)*
- *Surveys/questionnaires of pupils, parents/carers and staff*

Scope of the Policy

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.

It also covers best practice in remote learning situations during periods of extended school closure.

The Education and Inspections Act 2006 empowers Principals 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 Behaviour Policy. 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.

Other relevant linked policies: HEALTH AND SAFETY POLICY; E-SAFETY AND ICT ACCEPTABLE USE POLICY; ICT CODE OF CONDUCT FOR STAFF

Roles and Responsibilities

The following section outlines the safeguarding and online safety roles and responsibilities of individuals and groups within OLA:

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 Body/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

Principal and Leadership Team

- The Principal 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 Principal 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 Principal and Chief Operating Officer are responsible for ensuring that the Online Safety Lead (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 Principal 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead (DSL)

- leads the Online Safety meetings as part of the wider WSST meetings
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school 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 taking place.
- 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 meetings to discuss current issues, review incident logs and filtering/change control logs
- reports regularly to Leadership Team
- incidents dealt with by the Online Safety Lead supported by the Leadership Team and Year Tutors.

During periods of remote learning (such as COVID-19 pandemic): *The Leadership Team and DSL are in regular contact with each other and key members of staff*

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.

Those with technical responsibilities are responsible for ensuring:

- that OLA's technical infrastructure is secure and is not open to misuse or malicious attack

- 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
- the filtering policy is applied and updated on a regular basis and that 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 Principal and Leadership Team and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in OLA policies

Teaching and Support 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 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
- all digital communications with pupils/parents/carers should be 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

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. Integration of Class harts Safeguarding module is currently in training phase and will be launched with staff at the start of the Trinity term to allow all safe to report any concerns remotely.*

Designated Safeguarding Lead

Technology provides additional means for safeguarding issues to develop. Should be trained in online safety issues and be 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. The Deputies for the various parts of the school will take over should the DSL become unwell. Any incidence of peer-on-peer 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.*

In a pandemic situation where staff and pupils are working remotely, it is not 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 **principal** 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 the school or college.*

DSL training is very unlikely to take place for the period COVID-19 measures are in place, however no members of the Safeguarding Team are due refresher training. Members of the team can take advantage of free online training. All existing OLA staff will already 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 the school or college, they should continue to be provided with a safeguarding induction. This will include being provided with the updated Child Protection Policy.

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 the monitoring the Online Safety Policy including the impact of initiatives. The WSST will also be responsible for regular reporting to the Governing Body.

Members of the WSST will assist the Online Safety Lead 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

***During periods of remote learning (such as COVID-19 pandemic):** 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 **AHP** is responsible for dealing with any incidents of online misbehaviour.*

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 peer-on-peer 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.*

Attendance*: Pupils are expected to register for morning and afternoon remote learning sessions. OLA is not required to complete a day-to-day attendance process for DfE. OLA is providing provision for key worker and vulnerable children and the DSL will follow up on any child that was expecting to attend, who does not. 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 has confirmed that emergency contact numbers are correct and asked for any additional emergency contact numbers where they are available. 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 this difficult period 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.

Parents/carers

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

During periods of remote learning (such as COVID-19 pandemic): *Any incidence of peer-on-peer 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.*

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 AUA before being provided with access to school systems.

Policy Statements

Education – Pupils

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, this section includes additional information as outlined in ***COVID-19: Safeguarding in schools, Colleges and other providers (27 March).*** *It states that despite schools operating in a remote environment, 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*

The following documents have also been consulted.

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
Safer Remote Learning and here
Templates for online safety
London Grid for Learning – Use of videos and Livestreaming

During periods of remote learning*, it may be deemed necessary to revisit aspects of this appendix with pupils.*

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

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. 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 should be provided as part of Computing/PHSE/other lessons and should be regularly revisited
- Key online safety messages should be 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 should be 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 should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be 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 should be 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 should 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 should be 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.

Education – Parents/carers

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.

***During periods of remote learning**, it may be deemed necessary to revisit aspects of this appendix with parents.*

OLA will therefore 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)*

Education – 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*

Education & Training – Staff/Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- 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 Online Safety Lead 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 Online Safety Lead will provide advice/guidance/training to individuals as required.

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 all staff: Negative experiences and distressing life events, such as the current circumstances, 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 in the current circumstances is provided by:

- regular check-ins from Year tutors
- weekly online wellbeing questionnaires
- follow up on low questionnaire scores by DSL, AHP and Year Tutors
- Guidance information distributed to parents through ***connectED parent resource***
- Guidance information distributed to staff through ***connectED staff resource***
- 'Feel Good Friday' activities

We are using the guidance supplied in mental health and behaviour in schools.

Training – Governors

Governors/Directors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. 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

Infrastructure

OLA will be responsible for ensuring that the infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- OLA's technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to OLA's technical systems and devices.
- All users (at KS3 and above) will be provided with a username and secure password by our ICT Technician 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 "master/administrator" passwords for OLA systems, used by the Network Manager must also be available to the *Principal* and kept in a secure place (e.g. a safe)
- Our ICT contractors are 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
- 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

- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- OLA has provided enhanced/differentiated user-level filtering allowing different filtering levels for different ages/stages and different groups of users
- 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.
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed.
- 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.
- 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.
- 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.
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on school devices.
- 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.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

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 use of policies, notices and records.
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the 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

Communications (when working from site and remotely)

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 KS1 and 2, 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.

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.

OLA is doing all it reasonably can to keep all children safe during remote learning. 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 Behaviour Policy. 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

As necessary, this support is shared with parents and carers.

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 Junior 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.

Online Remote Learning Responsible User Agreement (for Junior and Senior)

Expectations and requirements during temporary closure of school

Rules

These rules are a basic outline of the principles for online working. Please refer to the Remote Learning Document for full details of online protocols when using video conferencing tools such as Zoom.

- ✓ I will only use technology for school purposes as directed by my teacher
- ✓ I will only use technology when there is an adult in the house and they know I am using it
- ✓ I will not reveal my passwords to anyone
- ✓ I will be responsible for my behaviour and actions when using technology, including the resources I access and the language I use
- ✓ I will make sure that all my communication with students, teachers and others using technology is responsible and sensible
- ✓ I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher or my parent
- ✓ I will not record or take photos/screenshots of my classmates or teachers during video sessions
- ✓ I understand that when using applications provided by the school that my use can be monitored and logged and be made available to my teachers
- ✓ I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent may be contacted
- ✓ I understand that zoom is an extension of the classroom and that I should conduct myself as I would in a classroom environment. This includes:

    - *Taking part in a zoom meeting in an environment that is safe, quiet and free from distractions (preferably not a bedroom)*
    - *Being on time for the virtual meeting*
    - *Being addressed appropriately for learning*
    - *Remaining attentive during sessions*
    - *Interacting patiently and respectfully with your teachers and peers*
    - *Not recording each other's online interactions*
    - *Finishing the session when your teacher instructs you to do so*

Mobile Technologies

OLA does not have a BYOD Policy and does not supply devices to pupils. 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

Use of digital and video images

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. 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 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.

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

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 accounts. 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:

- 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

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.

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.

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, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 N.B. Schools/academies should refer 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
	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	

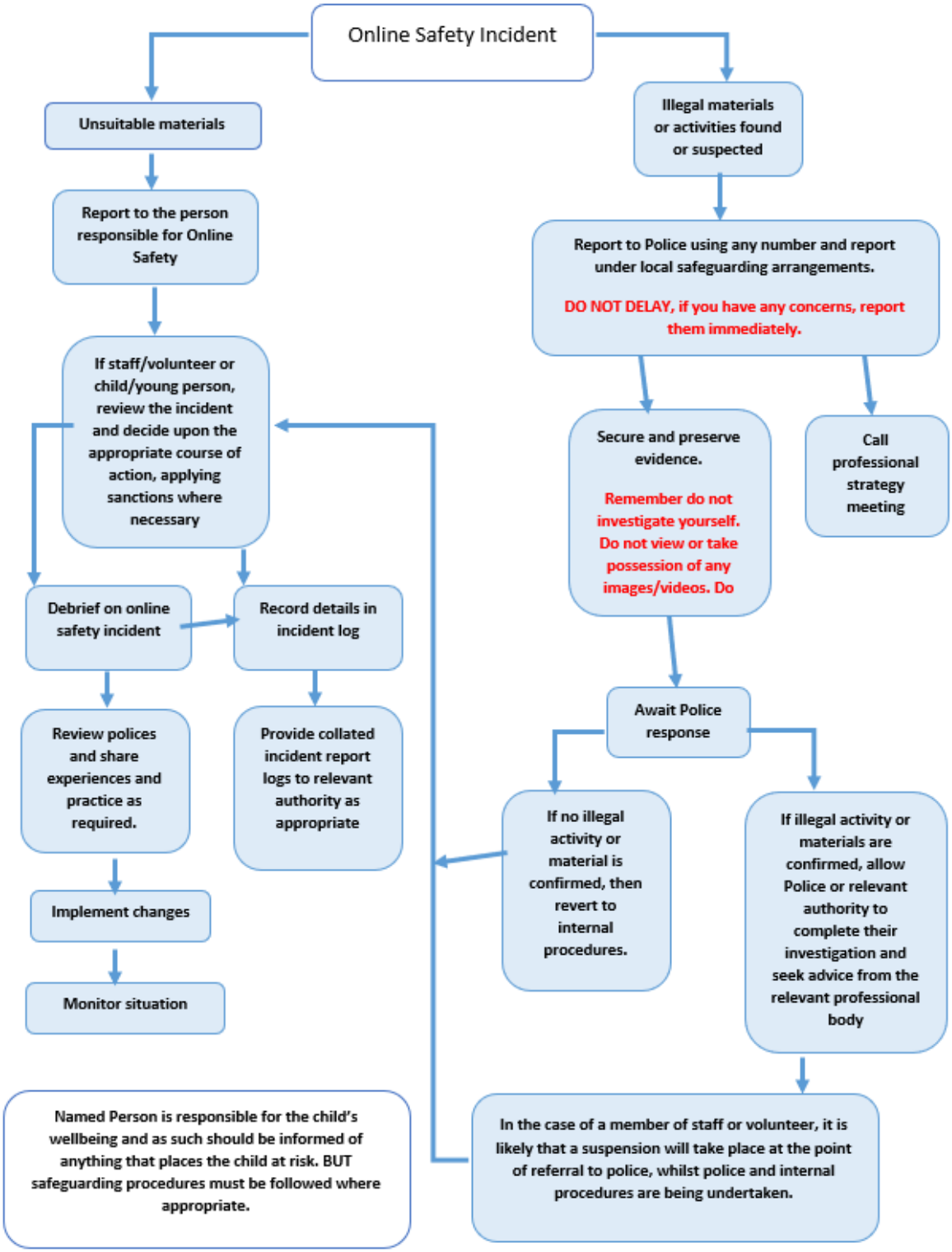
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary 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 and appendix) 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								

Appendices

Student/Pupil Acceptable Use Agreement Template – for older pupils

OLA policy

This document sits alongside OLA's E-SAFETY AND ICT ACCEPTABLE USE POLICY. Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe access to these digital technologies.

This acceptable use agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

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 OLA 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 that 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 OLA's 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 try (unless I have permission) to 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 use OLA's 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 OLA:

- 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 OLA, 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.
- I will only use social media sites with permission and at the times that are allowed

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 OLA 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 loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page 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 and devices.

Student/Pupil Acceptable Use Agreement Form

This form relates to the pupil acceptable use agreement; to which it is attached.

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

- I use the *OLA* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.

- I use my own equipment out of the school in a way that is related to me being a member of the OLA community e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Name of Pupil: .....

Group/Class: .....

Signed: .....

Date: .....

Parent/Carer Countersignature (optional)

Student/Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation/KS1/KS2)

This document sits alongside OLA's E-SAFETY AND ICT ACCEPTABLE USE POLICY and JUNIOR SCHOOL (including EYFS) COMPUTING AND INFORMATION AND COMMUNICATION TECHNOLOGY 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): .....

Signed (parent): .....

Parent/Carer Acceptable Use Agreement Template

This document sits alongside OLA's E-SAFETY AND ICT ACCEPTABLE USE POLICY. Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupils will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the s*tudent/pupil* acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name: .....

Student/Pupil Name: .....

As the parent/carer of the above *students/pupils*, I give permission for my son/daughter to have access to the internet and to ICT systems at school.

Either: (KS3and above)

I know that my son/daughter has signed an acceptable use agreement and has 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.

Or: (KS1/2)

I understand that the school 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 the school 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 the school 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 the school 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 the school if I have concerns over my child's online safety.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)
Who will have access to this form.
Where this form will be stored.
How long this form will be stored for.
How this form will be destroyed.

Signed: .....

Date: .....

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use 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 **delete as relevant** first name/initials will be used.

The school will comply with the Data Protection Act and request parent's/carers permission before taking images of members of the school. 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.

As the school is collecting personal data by issuing this form, it should inform parents/carers as to:

This form (electronic or printed)	The images
Who will have access to this form.	Where the images may be published. Such as; Twitter, Facebook, the school website, local press, etc. (see relevant section of form below)
Where this form will be stored.	Who will have access to the images.
How long this form will be stored for.	Where the images will be stored.
How this form will be destroyed.	How long the images will be stored for.
	How the images will be destroyed.
	How a request for deletion of the images can be made.

Digital/Video Images Permission Form

Parent/Carers Name:..... Student/Pupil Name:.....

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
Insert statements here that explicitly detail where images are published by 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: .....

Use of Cloud Systems Permission Form

The school uses **insert cloud service provider name** for *pupils/students* and staff. This permission form describes the tools and pupil/student responsibilities for using these services.

The following services are available to each *pupil/student* as part of the school's online presence in **insert cloud service provider name**

Using **insert cloud service provider name** will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate via email with other pupils and members of staff. These services are entirely online and available 24/7 from any internet-connected computer.

The school believes that use of the tools significantly adds to your child's educational experience.

As the school is collecting personal data and sharing this with a third party, it should inform parents/carers about:

This form (electronic or printed)	The data shared with the service provider
Who will have access to this form.	What data will be shared
Where this form will be stored.	Who the data will be shared with
How long this form will be stored for.	Who will have access to the data.
How this form will be destroyed.	Where the data will be stored.
	How long the data will be stored for.
	How the data will be destroyed.
	How a request for deletion of the data can be made.

Do you consent to your child to having access to this service? Yes/No

Student/Pupil Name: ..... Parent/Carers Name: .....

Signed: ..... Date: .....

Staff (and Volunteer) Acceptable Use Policy Agreement Template

OLA Policy

This document sits alongside OLA's E-SAFETY AND ICT ACCEPTABLE USE POLICY and ICT CODE OF CONDUCT FOR STAFF. New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This acceptable use policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that OLA systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy 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. I recognise the value of the use of digital technology for enhancing learning and will ensure that students/pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that OLA will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *OLA* systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students/pupils and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of OLA:

- When I use my mobile devices in school, I will follow the rules set out in this agreement, in the same way as if I was using *OLA* equipment. I will also follow any additional rules set by the *OLA* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the OLA ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, 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 ensure that my data is regularly backed up, in accordance with relevant OLA policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or 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 not try (unless I have permission) to 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 machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in OLA policies.
- I will not disable or cause any damage to OLA equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School/LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based documents containing personal data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- 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 I am responsible for my actions in and out of OLA:

- I understand that this acceptable use policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the

premises and my use of personal equipment on the premises or in situations related to my employment by the school

- I understand that if I fail to comply with this acceptable use agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

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.

Staff/Volunteer Name: .....

Signed: .....

Date: .....

Acceptable Use Agreement for Community Users Template

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

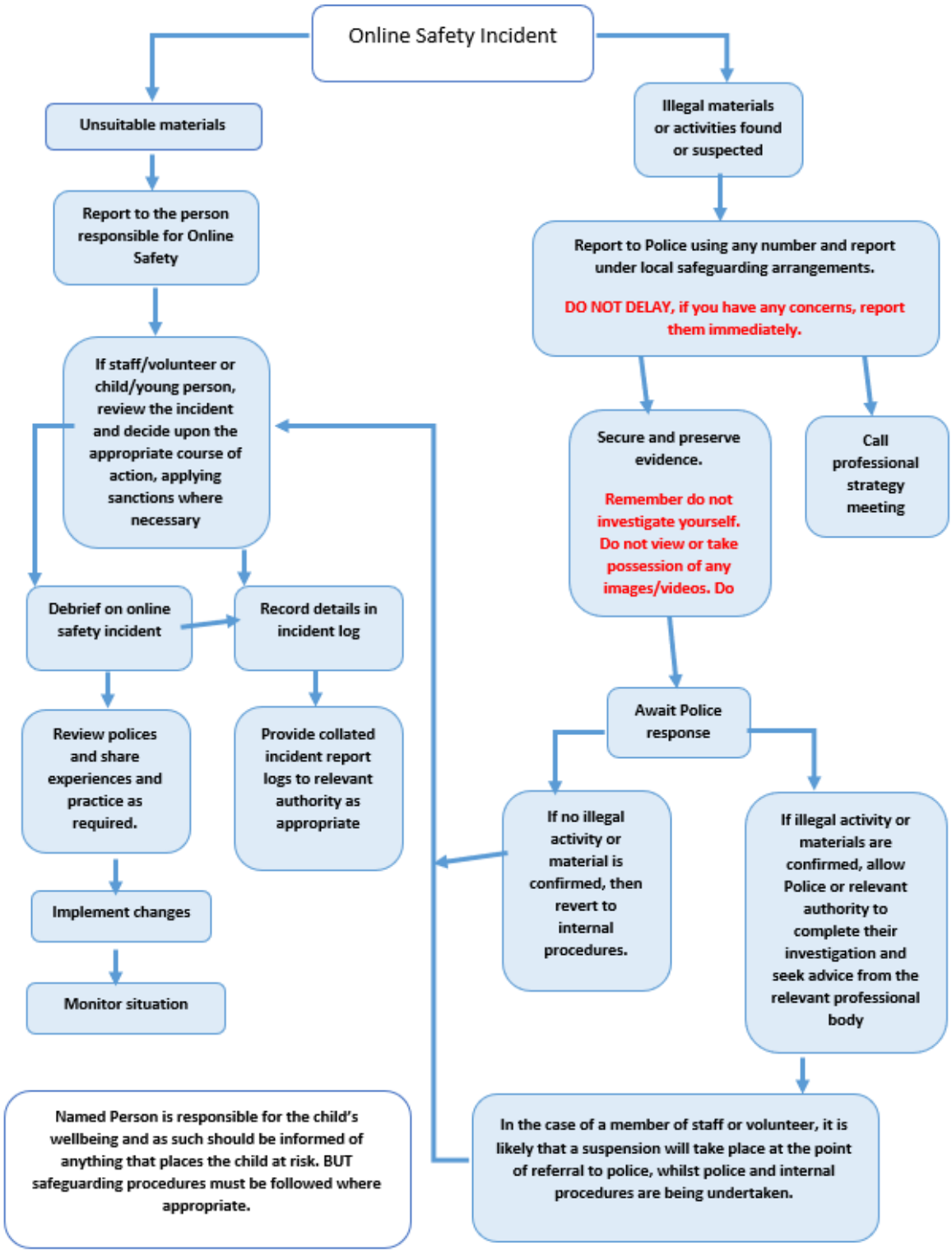
I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

As the school is collecting personal data by issuing this form, it should inform community users about:

Who will have access to this form.	How this form will be destroyed.
Where this form will be stored.	How long this form will be stored for.

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

Responding to incidents of misuse – flow chart



Record of reviewing devices/internet sites (responding to incidents of misuse)

Group: .....

Date: .....

Reason for investigation: .....

.....

.....

Details of first reviewing person

Name: .....

Position: .....

Signature: .....

Details of second reviewing person

Name: .....

Position: .....

Signature: .....

Name and location of computer used for review (for web sites)

.....

.....

Web site(s) address/device	Reason for concern

Conclusion and Action proposed or taken

Reporting Log

Group: .....

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Training Needs Audit Log

Group: .....

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

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

Glossary of Terms

AUP/AUA	Acceptable Use Policy/Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of National Crime Agency, UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family Online Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
SWGfL	South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for schools and other organisations in the SW
TUK	Think U Know – educational online safety programmes for schools, young people and parents.
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.
UKCIS	UK Council for Internet Safety
VLE	Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,
WAP	Wireless Application Protocol

A more comprehensive glossary can be found at the end of the UKCIS Education for a Connected World Framework