E-SAFETY AND ICT ACCEPTABLE USE POLICY (PUPILS)

DEFINITION

Information and Communications Technology (ICT) is a term used to include all forms of computing systems, telecommunications and networks. *Telecommunications* includes all methods of electronically communicating information, including data, text, pictures, voice and video.

AIM

To promote the use of ICT to facilitate and support learning, whilst informing pupils, parents and staff of the dangers as well as the benefits, and agreeing contracts for acceptable use. To bring the misuse of ICT, should it ever occur at home or at school, into the School's pastoral and disciplinary framework. To enrich learning for pupils.

1.0 SECURITY

1.1 All pupils are expected to take responsibility for their files in an age-appropriate way. In Early Years and Key Stage 1, children are taught to log on and the importance of remembering their password. In Key Stage 2 onwards, children are issued with individual passwords, which class teachers keep a record of. In the Senior School, all pupils are expected to take full responsibility for their passwords and files. Passwords should not be given to anyone and should be changed if it is suspected that someone else knows it. Every member of the School has a responsibility to protect the security and confidentiality of the School networks, therefore do not share passwords or access another person's work without permission.

1.2 Personal PDAs, digital cameras and computer hardware should not be brought into School unless absolutely necessary as part of learning support arrangements and with staff permission. At the Junior School, parents should liaise with class teachers to arrange this; class teachers will support children to store their equipment safely when not in use. In the Senior School pupils must make their own arrangements for their safe storage.

1.3 Pupils must not become involved in any inappropriate, anti-social or illegal behaviour involving the School computer systems.

1.4 All work is only secure and backed up if it is stored on the server.

1.5 Work may be shared with others using the subject folders in the shared area of the network or by email.

2.0 USE OF ICT EQUIPMENT

2.1 Any activity that attacks or corrupts the network or the computer systems is forbidden.

2.2 All computer equipment is the property of the School and should not be removed from the premises without permission.

2.3 Pupils must regularly (at least once a year) clear their personal area of the network of unnecessary files.

2.4 ICT equipment should be used for school-related purposes only.

2.5 Pupils are expected to behave sensibly when using ICT resources and also to log off when they have finished working and tidy the work space they were at.

2.6 Pupils activities on the computer systems may be monitored electronically.

Pupils must not:

- Create or store files that contain unsuitable language, images or discrimination of any kind.
- Download or use any unauthorised executable files on the network. This includes audio and video files.
- Connect their own computer hardware to the School network without permission.
- Use School equipment for any commercial purpose.
- Commit any copyright violations, e.g. copying music files.

Pupils' code of conduct:

- Food or drink should not be taken into any of the ICT suites or near any computer equipment.
- Bags should be left in the designated places in the ICT suites and not near or underneath workstations.
- Hands should be clean before handling computer equipment.
- Pupils should never run in the ICT suites and do not touch any leads or sockets.
- Work should be checked before printing to avoid excessive use of paper and printer toner.
- Problems with ICT equipment should be reported either to the Class Teacher (Junior School) or directly to the IT technician (Senior School) using the email: *helpdesk@olab.org.uk*

3.0 THE INTERNET

3.1 All members of the School community have access to the Internet for educational purposes. Internet content is filtered and access is monitored and websites visited are logged.

3.2 On-line games, chat or instant messaging are forbidden except when supervised by a member of staff.

3.3 Social networking sites are filtered – they may not be used in school.

3.4 Pupils should not use the Internet or email to arrange to meet someone they do not know.

3.5 Pupils should follow the School guidelines on copyright and plagiarism, which states that any image or passage of text copied from a public source such as the Internet or CD/DVD, should be properly acknowledged giving the site URL (if appropriate) and the author and the date.

Pupils must not:

- View, share, store, upload or download any offensive, obscene, indecent or menacing images, script or data.
- Post anonymous messages or pose as another person or promote physical harm to anything or anyone.
- Use the School computer systems for political purposes or advertising.
- Create, upload or download any computer virus.
- Use the Schools ICT equipment to gain or attempt to gain unauthorised access to any

other computer systems internally or externally.

- Use peer-to-peer services within the school.
- Do anything which would intentionally disrupt network security or communications.

If pupils come across a web site which they think might not be suitable, they should report it immediately to a teacher, giving the URL of the website - or email the information to the school using the email address: *helpdesk@olab.org.uk*

4.0 EMAIL

4.1 All pupils in the Senior School have a school email address which is to be used for school-related purposes only.

4.2 School email is filtered for viruses and spam.

4.3 Pupils are responsible for all emails sent or contacts made, including Internet activity resulting in email being received.

4.4 Pupils are advised not to provide their address, telephone number, photograph or other personal details to anyone they do not know personally.

4.5 Email folders should be checked regularly and messages deleted when no longer needed.

Pupils must not:

- Use the School email system for gambling, political purposes, advertising or personal financial gain.
- Send chain letters or spam.
- Send inaccurate, obscene, threatening, defamatory or racially offensive email, or harass or bully others or to commit crimes.

5.0 PHOTOGRAPHS

5.1 The school will use photographs of pupils from time to time, for example in newsletters, school magazines, press releases and the website. Parents who do not want their child's photograph to be used, should write to the Principal to let the School know. The policy is that generally only the pupil's first name will be used when photographs are used. Where a full name is needed, for example for press releases, the School will contact the parents to seek their permission.

5.2 Pupils are not permitted to take photos of other pupils or staff on school premises or on school outings, without permission from a member of staff and the person they are photographing. Pupils are not permitted to upload photographs of members of the school community onto any website without seeking advice and permission from a member of staff.

6.0 MOBILE PHONES

6.1 Since the school has a phone available for use by pupils who may need to contact parents, and messages from parents given to the office will always be passed on to pupils, the school recommends that mobile phones are not brought in to school. However, there is an understanding that a mobile phone may be needed after school hours and therefore, if a mobile phone is brought in to school, Senior School pupils must be responsible for keeping it safe and secure. The school will not be responsible for any personal electronic equipment which is damaged or lost by pupils and parents are advised to get appropriate insurance.

All mobile phones must be turned off in school. Junior School pupils who bring a phone to school must hand it in in the office in the morning, where it will be kept in a locked drawer until it is collected at the end of the school day.

6.3 Pupils found using a mobile phone without permission on the school premises or on school outings, will have it confiscated. For clarification, if a mobile phone is turned on, it will be deemed to be in use.

6.4 Confiscated phones will be returned to the pupil at the end of the day by the Principal's PA (Senior School) or the Head (Junior School), but a parent will be called in to school to retrieve the mobile phone if there is reason to believe that there may be offensive or compromising material which might endanger or offend the owner or others, or which has been obtained without the appropriate permission. The pupil and parent will either be asked to get it deleted or if there are serious concerns, the matter will be reported directly to the police. If a phone is confiscated more than twice in one term from a pupil, the parents will also be called in to school. A message will be sent home following any infringements of the rules with regard to mobile phone use, and after-school detentions, temporary or permanent exclusion from school may also be used depending on the frequency or severity of the rule infringement.

7.0 INTERACTIVE SOCIAL NETWORKING WEBSITES

7.1 Interactive websites such as *Facebook* are increasingly used by young people to communicate with each other. Many also use instant messaging facilities. Nationally, there has been growing concern about the evidence of misuse, including threats, abuse, bullying, racism, harassment and defamation. There is also awareness that what is placed on these websites is in the public domain and material that pupils write about themselves or others, however genuinely intended, may harm reputations or be regretted later for other reasons. As far as is possible, such websites are made *inaccessible* in school, but the misuse of such websites either at school *or* home, will come into the School's pastoral and disciplinary framework if it affects a member of the school's community.

7.2 **The following are NOT permitted**:

- Unless supervised by a member of staff, the Schools' ICT systems must not be used to create or publish web pages on interactive networking websites or other websites of a kind described above. Disciplinary action will be taken against anyone who breaks this rule.
- Complaints, gossip or rumour about the School or a member of the school community will be investigated. Where they relate to the use of websites, the School reserves the right to use inspection software to view web pages. This right will only be exercised when considered to be necessary and reasonable in the interests of welfare, and in each case a decision to view web pages will be balanced against the pupil's right to respect for private and family life.
- Pupils will be held *personally responsible* for all material they have placed on a website and for all material that appears on a website of which they are the host or account holder. Material of a threatening, abusive, bullying, racist, harassing or defamatory nature, whether placed during or outside school time (including the holidays) will be treated as a serious breach of school discipline.
- Pupils must expect to be dealt with seriously if they are responsible (in the sense

explained above) for material on their own or another website that is in breach of the terms and spirit of this policy or would be a breach of our school positive behaviour code in any other context.

- Pupils should regard it as their responsibility to report all misuse of networking websites of which they become aware. This may be done on a "no-names" basis provided sufficient information is given to enable the School to take action.

8.0 SANCTIONS

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

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

9.0 OTHER PROCEDURES

9.1 All pupils are taught about e-safety, reminded of the ICT policy and what is considered to be acceptable. They are responsible for their behaviour in respect of this policy. If there is any doubt about the meaning of any of the rules, then clarification must be sought from the Deputy Head or another member of the Leadership Team.

9.2 The School has the right to openly monitor the use of computer equipment and Internet and email systems to prevent them from being used inappropriately, and balances this against an individual user's right to privacy. The School reserves the right to examine and disclose any data on the School's network for the purpose of protecting property or ensuring the health, safety, discipline or security of any pupil or staff. This information may be used in disciplinary procedures.

9.3 Our Lady's Abingdon is registered as a "data controller" and in accordance with GDPR (May 2018) stores reasonable information about its pupils and staff.

Further information may be obtained by referring to:

- The Data Protection Act (1998)
- The Computer Misuse Act (1990)
- The Child Protection Act (2004)
- KCSIE (September 2018)
- Working Together to Safeguard Children (2018)
- The Electronic Communications Act (2000)