HARLINGTON LOWER AND SUNDON LOWER SCHOOL
ONLINE SAFETY AND ACCEPTABLE USE POLICY

Approved by Curriculum Trustee Committee: November 2022
Next review: November 2023

Senior Information Risk Owner (SIRO) – Miss Paulding
Asset Information Owners (AIO) - Miss Paulding, Mrs Cullis, Mrs Clarke and Mrs Churchill
Online safety Coordinator – Mrs Churchill

Introduction

Whilst exciting and beneficial both in and out of the context of education, much ICT (Information and Communication Technology), particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies. At School we understand the responsibility to educate our pupils on online safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

An online Safeguarding risk assessment has been completed and will be reviewed annually with this policy (appendix 1a).
When the annual Online Safeguarding risk assessment is completed, the Online safeguarding procedures will be reviewed (appendix 1b) and if necessary an online safety action plan completed. (appendix 1c)

1.Teaching and Learning

1.1 Why the Internet and digital communications are important

- The Internet is an essential element in life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

1.2 Internet use will enhance learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not. Pupils will be reminded of the Acceptable use agreement and computer suite rules at regular intervals. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience and how to evaluate Internet content. The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be taught the importance of cross-checking information before accepting its accuracy.

2. Managing Internet Access

2.1 Information system security

- School ICT systems security will be reviewed regularly following guidance issued by the LA/government.
- Virus protection will be updated regularly through automatic updates of ESET endpoint anti-virus.
- Passwords and network/MIS/school email user names will be kept safe and secure and changed regularly.

2.2 E-mail

- Staff are issued with GSuite email accounts, but may access personal mail accounts if required during break times or before/after school.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

2.3 Published content and the school web site

- An annual risk assessment will be undertaken by the Online Safety Co-ordinator and the SIRO. (see appendix 2)
- Staff or pupil personal contact information will not be published.
- The Online safety Co-ordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

2.4 Publishing pupil's images and work

- Parents sign an authorisation form when their child begins school, giving permission for images of their child (or their work) to be used on the website and on other publications e.g. weekly newsletter, village publications and local media. Where this permission is not granted, photos/work are never used.
- Photographs and images of pupils work will be used on the web site in line with government and Local authority guidance ie: If a photograph/work is used the pupils name will not be used. If the pupils name is used the photograph/work will not be used.

2.5 Social networking and personal publishing (e.g. blogging)

- Pupils will not have access to social network sites during school hours.
- Pupils and parents will be advised that the use of social network sites outside school must be made within the individual sites terms and conditions.
- Pupils will be advised through online safety lessons never to give out personal details of any kind which may identify them or their location.
- Staff, Trustees and pupils will be reminded to 'think before you post'. You lose control of text, images, and video recordings once they are posted in the public arena, even if you delete them. It is very difficult to know who has viewed them, including past, present and future employees, colleagues, pupils and parents. Items can also be copied, manipulated and redistributed, as well as remaining in search engine histories.
- Staff/Trustees using social networking sites should set the privacy levels on their accounts to maximum i.e only people on their friends' list should be able to view their pictures/private information etc.
- If you invite a parent (past or present) to be a friend because of common interests outside school (i.e neighbour, friend, relation etc) this is obviously your right. However, events/conversations within school MUST NOT be referred to.
- Staff and Trustees must be aware of their professional status and their school's reputation. Be respectful of other people's feelings and privacy. Only write comments in the public arena that you are prepared to say to some-one's face. Do not defame your place of work, any of your colleagues or any pupils - doing so goes against the Communications Act 2006, and you may be liable for disciplinary action by your employers.

3. Managing filtering

- If staff or pupils come across unsuitable on-line materials, the site must be reported to the Online Safety Coordinator. Sites can be referred to Schools Broadband for global blocking if required, or local blocking can be performed on-site through the server.

4. Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Pupils in the HASAT are not permitted to have mobile phones in school.

4.1 Mobile Phones/cameras

- Staff, Trustees and helpers may be required to take personal mobile phones on trips. These must not be used to capture images of pupils, and ideally, should not be used to make contact with parents or pupils. Emergency calls, where necessary should go through the school office.
- School digital cameras are provided.

4.2 Personal Electrical and Electronic Equipment

- Failure to maintain portable electrical equipment adequately is a major cause of electrical fires. Electrical equipment in schools will be maintained and PAT tested as appropriate and in accordance with the Electrical at Work Regulations 1989. Any personal electrical or electronic device brought into school is used at the owner's risk. It is the users duty to be responsible for the upkeep and protection of the device. HASAT will not be responsible for personal devices which are damaged or lost whilst at school. For staff, all plugs and connecting leads for personal devices must be PAT tested as part of the school's PAT testing annual programme.
- Access to the school wireless facility is in accordance with the school's Acceptable Use Policy.

5 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the relevant Data Protection Act.
- Any breaches of protecting personal data will be dealt with in line with the Trust's data breach policy.

6. Policy Decisions

6.1 Authorising Internet access

- All staff receiving a school laptop must sign the laptop loan agreement. (see appendix 3)
- All staff and Trustees must read and sign the relevant Acceptable Use Agreement before using any school ICT resource. (see appendix 4)
- Parents will be asked to sign the relevant Acceptable Use Agreement for their child to use the internet as part of the induction process. (see appendix 5)
- Pupils will be reminded of the Acceptable use Agreement at the beginning of each academic year.
- All users of the school computer system understand that the systems in place afford no privacy.

6.2 Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor Central Bedfordshire Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will carry out an online safety audit annually to establish if the online safety policy is adequate and that the implementation of the online safety policy is appropriate and effective through informal/formal monitoring. (see appendix 6)

6.3 Handling online safety complaints

- Complaints of Internet misuse will be dealt with by the Online Safety Coordinator or the SIRO.
- Any complaint about staff misuse must be referred to the SIRO.
- All incidents should be reported to the Online Safety Co-ordinator who will log details and consult with the SIRO. The Online safety incident log will be stored securely in the head teacher's office. (see appendix 7)
- The 'Flowchart for Managing an Online safety incidents' will be followed (see appendix 8)
- Complaints of a child protection nature must be dealt with in accordance with school and LA Child Protection Procedures.
- Pupils and parents will be informed of consequences for pupils misusing the Internet.
- Some incidents may need to be recorded in other places eg. a racist incident, CPOMS.

6.4 Community use of the Internet

- Any use of the school system by visitors will be bound by the terms and conditions in the Acceptable Use Agreement and will be monitored by the systems in place for pupils and staff.

7. Communications Policy

7.1 Introducing the online safety policy to pupils

- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- Online safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Online safety training will be embedded within the ICT scheme of work and the Personal Social and Health Education (PSHE) curriculum.

7.2 Staff and the Online Safety Policy

- All staff will be given the School Online Safety Policy and its importance explained.
- Staff are informed that network and Internet traffic is monitored and traced to the individual user and that there should be no expectation of privacy when using any school ICT equipment (including laptops used off-site).
- Any staff member with an online identity' (e.g. in social networking sites) will ensure that access to this information is kept private and not shared with pupils at school.

7.3 Enlisting parents' and carers' support

- Parents with any concerns about online safety are encouraged to contact the school for further guidance and support.
- Parents have the opportunity to attend Online Safety Information sessions in school and also at Parkfields Middle School.

8. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet.

- The Online Safety Co-ordinator will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that are not appropriate for their age through the use of appropriate firewalls.
- Cyber-crime can also affect adults and those who use technology daily to carry out their role can be at risk. To prevent this, schools should ensure where possible all staff, but as a minimum those staff who use the internet daily (including emails), receive regular Cyber Security training.

9. Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency disposal scheme. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

We support children in becoming well rounded individuals where they naturally demonstrate the values of the school in all aspects of their lives.