THE HARLINGTON AND SUNDON ACADEMY TRUST

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

Approved by Curriculum Trustee Committee: November 2023
Next review: November 2024

Additional information added on Pages 4 – 6 to reference updates from KCSIE 2023.

Senior Information Risk Owner (SIRO) – Miss Paulding
Asset Information Owners (AIO) - Miss Paulding, Mrs Cullis, Mrs Bork, 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.

10. Roles and responsibilies

3.1 The Board of Trustees

- The Board of Trustees board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- The Board of Trustees will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- The Board of Trustees board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The Board of Trustees board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The Board of Trustees should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The Board of Trustees board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:
  - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
  - Reviewing filtering and monitoring provisions at least annually;
  - Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
  - Having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 4)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the network manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, network manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The network manager

The network manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and regular monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 4), and ensuring that pupils follow the school's terms on acceptable use (appendix 5
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting it to the headteacher
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendx 5)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use in the volunteer handbook.

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

Safeguarding Risk Assessment Form **Reviewed by Head teacher and Online safety co-ordinator autumn 2023**
High Impact: Public exposure of restricted information leading to embarrassment, system downtime, or data corruption impacting learning & teaching.

E-Security and/or online safety issue (risk assess these plus others identified)	**Threat** (What could happen)	**Impact** [See definitions above] High: Score 3 Medium: Score 2 Low: Score 1	**Vulnerability** (What is it you do – or not do – that could lead to the threat materialising)	**Likelihood** High(3): next 6 month Medium(2): next 2 yrs Low(1): unlikely in next 2 years	**Total Score** (Impact x Likelihood; out of 9)	**Action Plan** (Either risk accepted OR actions to be taken to reduce risk)
Information (restricted/protected) taken out of school on laptop, email etc	Confidential information made available to public	3	Laptops and memory sticks containing confidential information being taken home.	3	9/9	All staff to be aware of and sign AUP. Staff meeting agenda item to discuss what can/can't be stored on laptops/sticks.
Use of mobile data storage e.g. memory sticks	Confidential information made available to public	3	As above.	3	9/9	No confidential /sensitive information to be stored on laptops/memory sticks.
Use of Internet for data transfer and communication	When replying to emails confidential/sensitive information may be unwittingly made available to others (eg in forwarded text)	1	Forwarding emails that contain confidential/sensitive information	2	2/9	Care when sending/replying to emails. Caution with attachments. Anycomms used for transferring pupil data.
Pupil gaining access to restricted or protected information	Pupils may read information about other children.	1	Laptop/staff drive left logged in with teacher not present.	1	1/9	Refer to AUP Laptops logged off when unattended. Staff drive logged off and back in as hls.
Remote access via school equipment or home computers	N/A					
Back up (storage)	If server crashed all stored data could be lost.	3	Irrregular backups and equipment maintenance	1	3/9	Laptops and Pc's back up to the servers. Each server has a 'mirror' back up, off site, on our partner school server. Ensure regular back ups of server to an external hardrive.
Password misuse or poorly managed	Passwords become know to non members of staff	2	Passwords not changed regularly.	2	4/9	Ensure staff change passwords regularly and advise network manager. Copy of passwords to be kept in safe in case of staff absence/illness.
Viruses and malicious software installs	Laptops/curriculum computers pick up virus. Data is lost.	3	Anti virus not updating. Allowing others to use laptop.	3	9/9	Check anti-virus updates. Refer to AUP re unauthorised use of staff laptops. Regular monitoring by Network Manager.
Inadequate staff and pupil training in e-security and online safety	Staff/pupils make mistake through lack of training. Children access staff drive.	2	Do not have regular online safety staff sessions. Computers left logged on to staff drive.	2	4/9	Add online safety as an agenda item on inset and training day agendas and staff. New staff to read Online safety policy and sign AUP. New pupils to sign AUP

Medium Impact: Exposure of protected information to a non-authorised third party, leading to outcomes listed above.
Low Impact: Internal exposure of information beyond authorisedindividuals leading to outcomes listed above.

Online Safeguarding Procedures: Reviewed by Head teacher and Online safety co-ordinator autumn 2023

Procedure	In Place	Partially in place	Not in place	Don't know	Actions for consideration
Roles and Responsibilities: SIRO appointed, IAOs identified and listed, technician responsibilities specified	✓				
1. Risk Assessment: Procedures established, assessments and remedial action plans documented	✓				
2. Information Classification: Table created and system for classification labelling established	✓				
3. Access Controls: *Systems access records* (who has access to what) and *Network security measures* established and implemented	✓				
4. Use of ICT Systems: AUP 'owned' by everyone. On-going education & training programme for everyone	✓				
5. Password Security: Minimum requirements in place	✓				
6. Incident Reporting: Procedure in use and monitored with action taken as necessary	✓				
7. Starters and Leavers: Procedures established and active for both staff and pupil records	✓				
8. Remote Access: Minimum requirements in place			✓		No remote access available
9. Technical Security: Minimum requirements in place	✓				

Online Safety Action Plan (January 2010 – November 2010 This appendix reviewed autumn 2023)

What will be done	*Resource Implications*	*Target Date(s)*	*Indicator of Success*	*Person Responsible*	*Date completed*
Write an online safety policy With pupil and staff acceptable use agreements	Time	**Jan 2010**	Policy written	Network Manager	**Jan2010**
Create an incident log,	Time	**Jan 2010**	Incident log created and appendix in online safety policy	Network Manager	**Jan 2010**
Complete online safety risk assessment	Time	**Spring 2010**	Online safety risks identified by SLT	SLT and Network Manager	**May 2010**
Complete information classification table	Time	**Spring 2010**	School information classified under levels of restricted, protected and public. Staff aware of classifications	SLT and Network Manager	**May 2010**
Appoint SIRO, IAO's and safety coordinator	Time	**Jan 2010**	SIRO, IAO's and safety coordinator in place and staff aware	SLT and Network Manager	**Jan 2010**
Memory sticks need encrypting	Cost of encryption	**Spring 2010**	Encryption in place and being used	Network Manager	**Not required all staff aware of online safety issues regarding memory sticks**
Governors to ratify online safety policy	Agenda item at Governors meeting	**Autumn 2010**	Ratified policy in place	Head teacher and Governors	**Autumn 2010**
Staff/Gov. online safety training	Time	**Spring 2010**	Staff/Govs aware of online safety issues	Network Manager	**Spring 2010**
Staff/Gov to sign AUP	Agenda item at staff/Gov meeting	**Spring 2010**	Completed AUPs	Network Manager	**Spring 2010**

THE HARLINGTON AND SUNDON ACADEMY TRUST

Online safety policy appendix 2

Website Risk Assessment

	Yes	No	Comments
Does the site market the school in a positive way	✓		
Is our mission and ethos clear	✓		
Has the content been considered for good taste and dignity	✓		
Can any child be identified through the site			
Is their any risk to members of staff	✓		
Are any children or staff named	✓		Names not linked to any photographs in line with online safety policy
Have all photo image names been checked	✓		
Is the content of good quality and up to date	✓		
Are any email addresses other than the school's on the site		✓	
Have external links been checked	✓		
Have we considered copyright issues	✓		
Have we considered data protection issues	✓		
Can any information on the site be deemed defamatory		✓	

The risk assessment has been carried out

By the Head Teacher and On-line Safety co-ordinator Date autumn 2023

Laptop Loan Agreement

A laptop computer will be loaned to you while you remain employed at the school. While the laptop is in your care the following items should be noted:

1. The Laptop remains the property of Harlington Lower or Sundon Lower School and is only for the use of the member of staff it is issued to.
2. The school insurance only provides cover while the laptop is on the premises.
3. Staff will need to insure the laptop on their own household insurance, whilst in the home and in transit, for standard and accidental risk.
4. Only software licensed by the school, authorised by the Headteacher and installed by the school's network manager may be used.
5. Anti-Virus software is installed and must be updated on a weekly basis. The network manager will advise on the routines and schedule of this operation.
6. Should any faults occur the school's network manager must be advised as soon as possible so that he/she may undertake any necessary repairs.
7. Any telephone charges incurred by staff accessing the Internet from home are not chargeable to the school.
8. LEA and school policies regarding appropriate use, data protection, computer misuse and health and safety must be adhered to by all users of the laptop.

Print Name……..

Signature……..

Acceptable Use Policy: Staff, Trustees, helpers and visitors

Computing and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff, trustees, helpers and visitors are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Online-Safety co-ordinator or the Head Teacher.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to pupils.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head Teacher. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, use of mobile technologies and use of social networking sites, both in school and outside school, will not bring my professional role or the school's reputation into disrepute.
- I will support and promote the school's online safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.
- I will be responsible for any personal electronic device that I bring into school.
- I will make any plugs and connecting leads for personal devices available for PAT testing.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ……

Full Name ……(printed)

Job title ……

Pupil Acceptable Use Policy/ Online safety Rules and Photograph/Video Permission

I agree that I will:

- Treat equipment with respect.
- Always keep my passwords a secret.
- Only access my own work/folder.
- Not tell anyone about myself online (eg: my name, home address or school name, school address etc).
- Tell an adult if anything online or in a message makes me feel scared or uncomfortable.
- Make sure all messages I send are polite.
- Follow the SMART rules for using the internet.

SAFE - Keep safe by being careful not to give out personal information when you're chatting or posting online. Personal information includes your email address, phone number and password.

MEETING - Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.

ACCEPTING - Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems – they may contain viruses or nasty messages!

RELIABLE - Someone online might lie about who they are and information on the internet may not be true. Always check information with other websites, books or someone who knows. If you like chatting online it's best to only chat to your real world friends and family

TELL - Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried, or if you or someone you know is being bullied online.

We appreciate that children will have different levels of understanding regarding these rules. Therefore we will discuss these rules regularly with the children to build their understanding as they progress through the school.

Child's name/signature……

Class……

School……

Date……

Parent/ carer signature

I have understand the above acceptable use policy and online safety rules and agree to support the safe use of technology at School.

I do / do not want my child to take photographs/video and be included in photographs/video taken at school. (these photographs will be used in displays, for assessment, in school publications, on the school web site and in local media)

Parent/ Carer Signature …….

Online Safety policy appendix 6

Online Safety Audit

Reviewed autumn 2023

When discussing and planning online safety there are a number of key aspects to consider. This audit should be reviewed yearly by the Governors, Head teacher and Online Safety Co-ordinator to ensure that online safety is a priority for our school.

The Designated Senior Person for Safeguarding is: Harlington: Mrs Tina Edmonds (DSL), Mrs Sharon Carter (deputy), Sundon: Mr Richard Kingham (DSL), Miss Sarah Sanby (deputy) HASAT: Miss Victoria Paulding (deputy), Mrs Jennie Churchill (deputy and CPOMS administrator)	
The Senior Information Risk Owner (SIRO) is: Miss Paulding	
The Online safety Coordinator is: Mrs Jennie Churchill	
Is the schools online safety policy reviewed yearly in line with Government and Local Authority guidance	✓
Staff, governors and visitors are expected to sign an 'Acceptable Use Policy' (AUP).	✓
Parents/pupils are expected to sign an 'Acceptable Use Policy' (AUP).	✓
Online safety rules are discussed regularly and displayed throughout the school.	✓
All staff consistently apply the online safety policies and rules.	✓
Clear and appropriate sanctions are applied if any member of the school community does not follow the AUP.	✓
All users are aware that the schools ICT systems are regularly monitored and any misuse will be followed up.	✓
Internet access is provided by an approved educational internet service provider and complies with the DCSF requirements for safe and secure access.	✓
The policy is available on the: learning platform and the school network. Hard copies can be obtained from the office.	

Online Safety Incident Log

Details of ALL online safety incidents to be recorded by the Online Safety Coordinator.
This incident log will be monitored termly by the Senior Information risk Officer (SIRO).
Any incidents involving racist/child protection issues should also be reported to the Designated teacher.

Date & Time	Name of pupil or staff member	Details of incident (including evidence)	Actions and reasons

Flowchart for managing an online safety incident.