HERRIES PREPARATORY SCHOOL

7h E-SAFETY (ACCEPTABLE USE) POLICY

Acceptable User and Information Security Policy for Staff

POLICY REVIEWS
September 2020 Rob Grosse
July 2020 FL
September 2019 Fiona Long, Andy Taylor and Katrina Sands to add incident log and form
September 2018 Fiona Long, Andy Taylor and Katrina Sands
December 2016 Sophie Green, Andy Taylor and Katrina Sands
May 2016 Sophie Green and Andy Taylor
February 2013 Sophie Green and Catherine Heron
January 2012 Sophie Green and Maureen Dimishky

Herries Preparatory School acknowledges the assistance provided by guidance documents prepared by the following public bodies:

• Teaching online safety in school. Guidance supporting schools to teach their pupils how to stay safe online, within new and existing school subjects. June 2019

• The Department for Education (DfE)
• The Independent Schools Inspectorate (ISI)

Education for a Connected World - A framework to equip children and young people for digital life:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759003/Education_for_a_connected_world_PDF.PDF

This policy also relates to Early Years Foundation Stage.

Policies and Documents linked to:
• ICT Agreement for Pupils
• 7g Images of Children Policy
• 7a Safeguarding and Child Protection Policy
• 10a Anti-Bullying Policy
• Data Protection GDPR Policy
• Employee Handbook

1. Aim of the Policy

The aim of this policy is to:

a. Ensure that Herries Preparatory School (the School) complies with its obligations under the Data Protection Act 2018 (the Act). This policy is aimed at all staff including temporary staff, agency workers, volunteers and all other people when

working in or for the School (whether directly or indirectly) and also applies to Governors.

b. Protect the good reputation of the School and support and enable effective use of ICT technology.

c. Set out the key principles expected of all members of the School community with respect to the use of ICT-based technologies.
Whilst the majority of this policy relates to the use of ICT, Section 4 (Information Security) also deals with information held in paper / hard copy.

d. Safeguard and protect children and staff.

e. Assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.

f. Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.

g. Have clear structures to deal with online abuse such as cyber-bullying which are cross referenced with other School policies.

h. Ensure that all members of the School community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

i. Minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

Breach of this policy

• Any breach of this policy will be taken seriously and may result in disciplinary action.

• A member of staff who deliberately or recklessly discloses Personal Data held by the School without proper authority is also guilty of a criminal offence and gross misconduct. This could result in summary dismissal.

Acceptable User and Information Security Policy for Staff

2. Expected Conduct

Staff :

a. Are responsible for reading the School's ICT-related policies and using the School ICT systems accordingly, including the use of personal mobile devices and digital cameras.

b. Must ensure that their use of the School ICT systems does not compromise the security of the network.

c. Must only connect to a device that has not been provided by the School when certain that doing so will not represent a security risk.

d. Are responsible for using the School ICT systems in accordance with this Acceptable User Policy.

e. Must use appropriate language when communicating by e-mail both internally and externally and when working online and using School devices. Staff should be aware that emails and Internet use is monitored by the school's own software for inappropriate text and content.

3. Incident Management

a. Complaints of cyber-bullying are dealt with in accordance with our Anti-Bullying Policy.

b. Complaints related to safeguarding and child protection are dealt with in accordance with the School's safeguarding procedures.

c. All incidents and complaints relating to e-safety and unacceptable Internet use will be reported using the 'E-Safety Incident Report Form'. An electronic version of this is available in Staff Common on the school system (see Appendix 1). This will be passed on to the Headteacher and the ICT Network Manager at ActiveIT. These will be stored securely in the Headteacher's office.

Incidents of inappropriate language and/or Internet use will be captured by the school's own software and reviewed.

d. Matters relating to a member of staff will be referred to the Headteacher for action.

e. Incidents involving the Headteacher will be referred to the Chair of the Board of Governors.

f. E-safety incidents involving safeguarding issues will be reported to the Designated Lead.

g. If a pupil or teacher accidentally opens a website that has content which is distressing, upsetting or inappropriate to the pupils' age, teachers should immediately close the screen and reassure pupils that they have done nothing wrong. The incident should be reported to the ICT Network Manager, including details of the website address and URL.

h. If a member of staff witnesses misuse of ICT by a colleague, they should report this to the Headteacher immediately. A note of any action should be recorded on the E-safety Incident Report Form.

i. All E- safety incidents relating to pupils should also be recorded on the 'E-safety Incident Log' available on the 'E-safety' folder in Staff Common on the school system(see appendix 2).

Any incidents relating to a member of staff will also be monitored and recoded as required by the Headteacher.

j. Under its 'Prevent Duty', the school recognises its responsibility to prevent children from being drawn into terrorism and becoming radicalised. The internet and social media has become a major factor in the radicalisation of young people. The school teaches online safety and has appropriate filtering software in place.

Any incidents or concerns staff have about pupils viewing online material relating to radicalisation should be reported to the DSL in line with the school's safeguarding procedures.

4. Information Security

a. Information security is the most important aspect of data protection compliance. Most of the fines under the Act relate to security breaches, such as leaving an unencrypted memory stick in a public place, sending sensitive documents to the wrong recipient, disposing of confidential documents without shredding them first or accidentally uploading confidential information to the web.

b. Under the Act, Personal Data is:

• Personal information that has been, or will be, word processed or stored electronically (e.g. in computer databases and CCTV recordings). If a record containing Personal Data is held on a computer then it will be covered by the Act. This is the case regardless of how the information is held. For example Personal Data stored in an email, in a spreadsheet or on a smartphone, are all caught by the Act.

• Personal information that is, or will be, kept in a file which relates to an individual or in a filing system that is organised by reference to criteria which relate to the individuals concerned (e.g. name, department, pay scale etc). Some paper records are not covered by the Act although there are so many exceptions that best practice is to treat all paper records as being covered.

• Some health records prepared by a doctor, nurse or other health professional (even if not held on computer or held as part of an organised file).

c. The Act requires the School to take organisational measures (for example, ensuring that staff are trained on information security), and technical measures (for example, encryption, secure shredding etc) to ensure that Personal Data is kept secure.

d. Staff must ensure that their use of Personal Data is necessary and proportionate. For example, staff must not take Personal Data off School premises unless there is a genuine need (subject to the other provisions of this policy).

e. Staff should take all necessary steps to prevent unauthorised access to information held on the School's ICT systems. Extra care should be taken with data that is classified as Sensitive Personal Data under the Act. Sensitive Personal Data is information about an individual's racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or

mental health or condition, sexual life and information relating to actual or alleged criminal activity.

f. Staff must be very careful when sending correspondence containing Personal Data (e.g., sending an email, or sending documents by post). Staff should check at least three times that they have got the address correct. If the communication contains Sensitive Personal Data or is particularly confidential then staff should take extra precautions such as asking a colleague to check that the number / email address has been entered correctly.

g. Staff should not share the personal details of others without prior consent. This is particularly important when sending emails to multiple recipients. Bcc should be used to protect email addresses.

h. Staff must not use or leave computers, portable electronic devices or papers where there is a significant risk that they may be viewed or taken by unauthorised persons: staff should take reasonable steps to ensure that such devices are not be viewed in public, and they must never be left in view in a car, where the risk of theft is greatly increased.

i. Staff have their own unique username and private passwords to access School systems. Staff are responsible for keeping their password secure. In the unlikely event of password security being breached, users must immediately change their password and inform the Office. Staff must not share their passwords with anyone else.

j. Staff will be required to reset their passwords on a regular basis.

k. No PCs, including remote access sessions, should be left unattended and unsecured when a member of staff is logged in. To prevent unauthorised access, users must either logout or lock the screen when leaving the room by holding down the Ctrl+Alt+Delete keys and selecting ‘Lock this computer’.

l. Remote access via the School server is the preferred route for accessing School information at home. Staff must ensure that their use of the School ICT systems does not compromise the security of the network.

m. Staff must immediately report all security incidents, breaches and weaknesses, to the Headteacher. This includes anything which the member of staff becomes aware of even if they are not directly involved (for example, if a teacher notices that document storage rooms are sometimes left unlocked at weekends). Any loss or theft of the School’s data must also be disclosed immediately by reporting it directly to the Headteacher.

n. Printed material of a confidential nature, which links any pupil to the School, should be printed in a secure area.

o. Printed material of a confidential nature, which links any pupil to the School, should not be kept for longer than is necessary and be disposed of using a shredder.

p. Staff should exercise caution when opening e-mail attachments, as these may contain viruses. E-mails from unknown sources, or from known sources which seem

“out of character” should be treated with extreme caution. If in doubt, advice should be sought from the Network Manager at ActiveIT.

q. With regards to the security of Personal Data held in physical form (e.g. paper files) staff must:
• Ensure that any such records are kept under lock and key in a secure location.
• Take extra precautions in relation to any Sensitive Personal Data (as defined above), and any Personal Data which is particularly confidential, both of which should be stored in a storage room or in a strong cabinet (again under lock and key).
• Ensure that documents containing Personal Data are never left unattended on desks (unless the room is secure).

5. E-mail

The School:

a. Provides staff with an e-mail account for their professional use, and makes clear that personal e-mail should be sent through a separate account.
b. Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.

c. Will ensure that e-mail accounts are maintained and up to date.

d. Reports messages relating to or in support of illegal activities to the relevant Authority and, if necessary, to the Police.

e. Knows that spam, phishing and virus attachments can make e mails dangerous.

We use a number of technologies to help protect users and systems in the School, plus direct e-mail filtering for viruses. Finally, and in support of these, filtering monitors and protects our Internet access to the World Wide Web.

f. Staff only use the School’s e-mail systems for professional purposes.

g. Use of external personal e-mail accounts should be limited during School hours.

h. Important e-mail communication with parents should be printed off and stored as a paper copy in the pupil’s file.

i. Staff know that e-mail sent to parents or an external organisation must be written carefully, and unless regarding a trivial matter, must gain approval and authorization prior to being sent, in the same way as a letter written on School headed paper.

j. the sending of multiple or large attachments should be limited, and may also be restricted by the provider of the service being used.

k. the sending of chain letters is not permitted.

l. embedding adverts is not allowed.

m. Where there is a direct link to a School e-mail account set up on a personal device, such as a mobile phone, this must be secured with a complex password.

n. Staff should note that the School may be required to disclose internal email communications to third parties, for example, if a parent makes a subject access request under the Act.

6. School Website

a. The Marketing Officer ensures that the quality of presentation is maintained. All Staff are expected to ensure that website content is accurate.

b. Uploading of information is restricted to our Marketing Officer, Secretary and Admin team.

c. The School website complies with the statutory DfE guidelines for publications.

d. Most material is the School's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status.

e. The point of contact on the website is the School address, telephone number and we use one e-mail contact address: reception&events@herries.org.uk

f. Photographs published on the web do not have full names attached.

g. We do not use pupils' names when saving images in the file names or in the tags when publishing to the School website.

h. We do not use embedded geo-data in respect of stored images.

7. Social Networking & Electronic Communication

School staff will ensure that in private and public use:

a. Staff demonstrate responsibility and act with integrity in relation to the School.

b. No direct reference should be made in social media to pupils, parents, carers or School staff.

c. They never engage in online discussion on personal matters relating to members of the School community.

d. Personal opinions should never be attributed to the School.

e. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

f. They do not communicate via personal e-mail addresses or accept friend requests from present or past pupils, who are unrelated, before they reach the age of 18.

g. They do not post comments or photographs which could bring into question their professional credibility.

h. Failure to comply with the policy relating to social media may result in disciplinary action. It must be assumed that whatever is written online anywhere cannot be deleted in the future.

8. Equipment and Digital Content Personal mobile phones and mobile devices

a. Mobile phones and personally-owned mobile devices brought in to School are the responsibility of the device owner. The School accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

b. Mobile phones and personally-owned devices will not be used in the presence of children during lessons, duties or other formal School time. They should be switched off or silent at these times. Failure to do this will result in disciplinary action.

c. Mobile phones may be used in an emergency when working at an off-site location.

d. No images or videos should be taken on mobile phones or personally-owned mobile devices unless with the permission of the Headteacher and then immediately downloaded to the central folder in Staff Common on the school system, then deleted. School-provided equipment should be used exclusively for this purpose.

e. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.

f. The School may in exceptional circumstances require access to your device (and any School related information contained in the device). If requested by the School, you must hand over the device and give the School any information (such as any password) necessary to access the device and remove any School Personal Data. The School would only make this request if investigating a serious incident or allegation such as a serious security breach involving the device.

g. Mobile phones and personally-owned devices are not permitted to be used in certain areas within the School site, e.g. changing rooms and toilets.

h. Only in emergencies will Staff be permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.

i. Staff have access to a School phone where contact with pupils, parents or carers is required.

j. Where staff members are required to use a mobile phone for School duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, then a School mobile phone will be provided and used. School mobile phones are kept in the school office and they will need to be signed in and out when staff leave and return to the school-site

k. In an emergency where a staff member does not have access to a School-owned device, they should use their own device and hide (by inputting 141 first) their own mobile number for confidentiality purposes.

Appendix 1

HERRIES PREPARATORY SCHOOL E-SAFETY INCIDENT REPORT FORM

Incident Report Form Compiled By: Name Title Date

Staff informed: *Name and Date* Headteacher Network Administrator ICT Co-ordinator Designated Lead for Safeguarding (must be informed in the event of a safeguarding concern) Other

Nature of Concern *(details of the events occurring including the location and the device(s) on which the incident occurred)*

Time and date of Incident:

Time and date the incident was logged:

Appendix 2

HERRIES PREPARATORY SCHOOL E-SAFETY INCIDENT LOG

Details of ALL e-safety incidents are to be recorded by the member of staff involved on this Incident Log found in the 'E-safety' folder in Staff Shared.

The member of staff also needs to record the details on an 'E-Safety Incident Report Form' which can also be found in the folder 'E-safety' on. Staff Shared The report form should be passed on to the Headteacher, the School's Network Manager ActiveIT, and also the Designated Lead for Safeguarding if there is a child protection concern.
This incident log will be checked & collated by the Headteacher. Any incidents involving Cyberbullying may also need to be recorded in the Anti-Bullying Log.

Date & time	
Name- pupil/staff	
Room and computer number	
Details	
Evidence	
Actions	
Explanation	

Outcomes	

STAFF ICT ACCEPTABLE USE POLICY AGREEMENT SCHOOL POLICY

New technologies have become integral to the lives of children 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 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 internet access at all times. This Acceptable Use Policy is intended to ensure:

• That staff will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• That the schools' ICT 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 ICT in their everyday work. The school will try to ensure that staff will have good access to ICT to enhance their work, to enhance learning opportunities for our young people and will, in return, expect staff to agree to be responsible users.

ACCEPTABLE USE POLICY AGREEMENT

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that children receive opportunities to gain from the use of ICT. I will, where possible, educate children in my care in the safe use of ICT and embed e-safety in my work.

Professional and personal safety:

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.
• I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, tablets, etc.) out of school.
• I understand that the school ICT 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.
• 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 will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Bursar.

I will be professional in my communications and actions when using school ICT 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 only use my personal equipment to record these images if it is password protected.
• I will not use chat and social networking sites in school in accordance with the school's policies.
• I will not engage in any on-line activity that may compromise my professional responsibilities or bring the school into disrepute.
• I will only communicate with pupil and parents / carers using official school systems. Any such communication will be professional in tone and manner.
• If the data on any device is breached I will report it to the Bursar.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

• When I use my personal hand held / external devices (Chrome books/iPads/PDAs / laptops / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school 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 open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
• I understand the importance of regularly backing up my work.
• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, racist 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 school policies.
• I will not disable or cause any damage to school 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 Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
• I understand that the data protection policy requires that any staff or young person's 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
• It is my responsibility to understand and comply with current copyright legislation.

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

• I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school, and my use of personal equipment in school or in situations related to my employment by the school.
• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors 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 ICT 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 Name

Signed

Date
