Haughmond Federation

E-Safety Policy

September 2017

(to be reviewed in September 2019)

Sundorne Infant School and Nursery

Harlescott Junior School

Contents Page

Responsibilities

The member of SLT team responsible for e-safety is Christine Maddox / Lisa Twidale

The governor responsible for e-safety is Roger Adams

The e-safety co-ordinator is Philippa Bentley / Alun Tombleson

The e-Safety co-ordinator is responsible for leading the e-Safety Committee, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the Federation community. They may also be required to deliver or arrange workshops for parents.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. There is a separate AUP for Ipads that staff read and sign, a copy of these are kept centrally. Examples of the AUPS used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip, or read to children by their teacher and explained within their class. These will then be signed by the children and copies kept in the office with the children's personal details. This can be found in appendix 2. AUP can be displayed in classrooms with the children's signatures.

AUP's will be reviewed annually. All AUP's will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

The Prevent duty

The Prevent duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the need to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and according to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff need to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

Internet searches for terms related to extremism
Visits to extremist websites
Use of social media to read or post extremist material
Grooming of individuals

All staff should be aware of the following

1. DfE Prevent duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel

The Prevent duty requires a schools monitoring and filtering systems to be fit for purpose.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then only the pupils first names should be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images.

Within federation each school sends their own letter to parents when the child eneters school on the registration form.

Staff should always use a school camera or Ipad to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The parental letter concerning AUP's includes a paragraph concerning posting photos on social networking sites (see appendix 2)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Mobile phones and other devices

All mobile phones (staff) should be switched to silent whilst on the school premises.

If a member of staff suspects that a mobile phone has been misused within the school then it should be confiscated but staff should not 'search' the phone. The incident should be passed directly to SLT who will deal the matter in line with normal school procedures.

Please see mobile phone policy for more details.

Use of e-mails

Pupils and staff should only use e-mail addresses that have been issued by the school and the e-mail system should only be used for school related matters. Pupils and staff are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Pupils and staff should never share passwords and staff must never let pupils use a staff log on. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector / screen will allow an image to remain on the screen and also allow a PC to be 'locked').

All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to used in school.

Reporting

All breaches of the e-safety policy need to be recorded in the Esafety reporting book that is kept in the general office or on CPOMS. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the Designated leads immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents that are of a concern under the Prevent duty should be referred to the designated lead immediately who should decide on the necessary actions regarding safeguarding and the Channel Panel.

Incidents which are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to SLT in the same way.

Allegations involving staff should be reported to the Headteacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the Local Authority should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Hector protector, Smart Crew videos, Ceop button, trusted adult, Childline.)

Infringements and sanctions

(generic age appropriate sanctions will apply for KS1.)

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the SLT.

The following are provided as exemplification only:

(a) Pupils

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites
- Use of Filesharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to SLT / Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to SLT / Class teacher / e-safety Coordinator / Headteacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site
2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988
- Bringing the school name into disrepute

[Possible Sanctions – Referred to Head Teacher / SLT / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:
1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

(b) Staff

Level 1 infringements (Misconduct)

- Excessive use of internet for personal activities not relating to professional development, e.g. online shopping, personal email, instant messaging, Social media etc.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license, e.g. installing unlicensed software on the network.

(Sanction – Headteacher. Warning given following HR policy.)

Level 2 infringements (Gross misconduct)

- Serious misuse of, or deliberate damage to any Federation / council computer hardware or software.
- Any deliberate attempt to breach data protection or computer security rules.
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent.
- Receipt or transmission of material that infringes of a copyright of another person or infringes the conditions of the Data Protection Act.
- Bringing the Federation name into disrepute.

(Sanction – Refer to Headteacher / Governors and follow school disciplinary procedures; Report to LA personnel / HR, report to police.)

Other safeguarding actions:

1. Remove the P.C. / Ipad to a secure place to ensure there is no further access.
2. Instigate an audit of ICT equipment by an outside agency, such as the Federations ICT providers – To ensure there is no risk of the pupils accessing inappropriate materials in the school.
3. Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of Gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that a member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – eg. class commendation for good research skills, Class Dojos, certificates for being good cyber citizens etc. Each year group co-ordinator will indicate these opportunities within the provided planning.

Social networking

Pupils

Pupils are not permitted to use social networking sites within school.

Staff

It is recognised that social networking sites have a major role to play in today's society. However, staff must be aware of the following:

Staff must not add pupils as friends on Social Networking sites.
Staff must not post pictures of school events without the Headteacher's consent.
Staff must not use Social Networking sites within lesson times.
Staff should review and adjust their privacy setting to give them the appropriate level of privacy.

Staff Communication

Staff should only communicate with pupils and parents through official channels. These include:

- Letters on Federation / School letter-headed paper.
- School telephone system.
- School provider mobile phone.
- School email system.

The following are excluded from the official channels:

- Social Networking sites.
- Gaming sites.
- Chatrooms.
- Personal mobile phones.
- Personal email addresses.

Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years.
b). Regularly auditing, review and revision of the Computing curriculum.
c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner.
d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc.

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
c). The Federation actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour.
d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

a). A planned programme of formal e-safety training is made available to all staff. Additionally, all staff will have CPD on the Prevent duty.
b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa.
c). An audit of e-safety training needs is carried out regularly and is addressed.
d). All staff have an up to date awareness of e-safety matters, the current Federation e-safety policy and practices and child protection / safeguarding procedures.
e). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy.
f). The culture of the Federation ensures that staff support each other in sharing knowledge and good practice about e-safety.
h). The school takes every opportunity to research and understand good practice that is taking place in other schools.
i). Governors are offered the opportunity to undertake training.

Parents and the wider community

Letters, leaflets and assemblies are available to parents about safety, and there is a page on the Federation's website offering information to parents.

Monitoring and reporting

a). The school network provides a level of filtering and monitoring that supports safeguarding.

b). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, CPOMS, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

c). The records are reviewed / audited and reported to:

- the Federation's Senior Leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

d). The school action plan indicates any planned action based on the above.

The Federation has in place the Local Authority filters blocking any websites that are not suitable for children. It is important that staff always check the websites they are using / search first as these filters are not always reliable.

The Federation's policy is to not let the children use the internet without close and careful adult supervision / monitoring. This is staff responsibility to risk assess each lesson.

Children use a safe search engine called 'Kidrex' which is safely filtered for children rather than using 'Google' or similar search engines.

Appendices

Appendix 1 – AUP's

AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- Never share passwords with people I don't know
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite
- show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher
- never agree to meet a stranger

Anything I do on the computer may be seen by someone else.

I am aware of the Acceptable Use Policy and how to stay safe when using a computer / laptop / Ipad.

I know that I must speak to my teacher if I am worried about anything online.

Signed _____

AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security
- make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission
- only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school
- only use email which has been provided by school
- never use a personal Social Networking site in school
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

Anything I do on the computer may be monitored by someone else.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I know that I must speak to a member of staff if I am worried about anything online.

Signed _____

AUP for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely
- respect the Federation's network security
- implement the Federation's policy on the use of technology
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site.
- only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer
- promote any supplied E safety guidance appropriately.

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling
- do anything which exposes others to danger
- post any other information which may be offensive to others
- forward chain letters
- breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission

- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor who takes responsibility for e-Safety
- an e-Safety Policy has been written by the Federation, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually
- the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately
- parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

Appendix 2 – Federation audit

Audit

The self-audit should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Shropshire guidance? Yes

Date of latest update (at least annual):	September 2017
The Leadership team member responsible for e-safety is:	Christine Maddox / Lisa Twidale
The governor responsible for e-Safety is:	Roger Adams
The designated member of staff for child protection is:	Christine Maddox / Lisa Twidale. Plus other leads
The e-Safety Coordinator is:	Philippa Bentley / Alun Tombleson
The e-Safety Policy was approved by the Governors on	6th October 2017
The policy is available for staff at:	Shared W drive
The policy is available for parents/carers at:	Federation website

Appendix 3 –

iPad Acceptable Use Policy for Haughmond Federation

The policies, procedures and information within this document applies to all iPads, or any other IT handheld device used in school. Teachers and other Federation staff may also set additional requirements for use within their classroom.

Users Responsibilities

Users must use protective covers/cases for their iPad. The iPad screen is made of glass and therefore is subject to cracking and breaking if misused:

*Never drop or place heavy objects (books, laptops, etc.) on top of the iPad.

*Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.

*Do not subject the iPad to extreme heat or cold.

*Do not store or leave unattended in vehicles.

*Users may not photograph any other person, without that persons' consent.

*The iPad is subject to routine monitoring by Haughmond Federation.

*Devices must be surrendered immediately upon request by any member of staff.

Users in breach of the Acceptable Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

*Haughmond Federation is not responsible for the financial or other loss of any personal files that may be deleted from an iPad.

Safeguarding and Maintaining as an Academic Tool

iPad batteries are required to be charged and be ready to use in school.

Syncing the iPad to iTunes or iCloud will be maintained by a School ICT Coordinator or Administrator.

Items deleted from the iPad cannot be recovered.

Memory space is limited.

Academic content takes precedence over personal files and apps.

The whereabouts of the iPad should be known at all times.

It is a user's responsibility to keep their iPad safe and secure.

If an iPad is found unattended, it should be given to the nearest member of staff.

Lost, Damaged or Stolen iPad

*If the iPad is lost, stolen, or damaged, the ICT Technician / Coordinator / Head Teacher must be notified immediately. iPads that are believed to be stolen can be tracked through iCloud.

Prohibited Uses (not exclusive):

Accessing Inappropriate Materials – All material on the iPad must adhere to the ICT Responsible Use Policy. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.

Illegal Activities – Use of the school's internet / e-mail accounts for financial or commercial gain or for any illegal activity.

Violating Copyrights – Users are not allowed to have music and install apps on their iPad for their own personal use.

Cameras – Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets, regardless of intent, will be treated as a serious violation. Images of other people may only be made with the permission of those in the photograph.

Posting of images/movie on the Internet into a public forum is strictly forbidden, without the express permission of the Teacher or in the case of staff use; a member of the Senior Leadership Team.

Use of the camera and microphone is strictly prohibited unless permission is granted by a teacher.

Misuse of Passwords, Codes or other Unauthorised Access: Users are encouraged to set a passcode on their iPad to prevent other users from misusing it.

Any user caught trying to gain access to another user's accounts, files or data will be subject to disciplinary action.

Malicious Use/Vandalism – Any attempt to destroy hardware, software or data will be subject to disciplinary action.

Jailbreaking – Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.

Inappropriate media may not be used as a screensaver or background photo.

Presence of pornographic materials, inappropriate language, alcohol, drug or gang related symbols or pictures will result in disciplinary actions.

If any individuals choose to connect their ipad to their home internet they should do so by taking into account the guidelines provided in the school's safety policy.

Haughmond Federation reserves the right to confiscate and search an iPad to ensure compliance with this Acceptable Use Policy.

Adult Users must read and sign below:

I have read, understand and agree to abide by the terms of the iPad Acceptable Use Policy.

Name

Signature
Date

Appendix 4 - Links

(a) Shropshire Council Education Improvement Service documentation

All EIS Service e-safety documentation can be found at:

https://www.shropshirelg.net/supporting-teaching-and-learning/e-safety/

(b) The Safe Use of New Technologies

The Safe Use of New Technologies report is summary of findings from OFSTED based on 35 e-safety inspections carried out in a range of settings.

http://bit.ly/9qBjQO

(**c) 360 degree Safe**

The policy guidance is based upon criteria with the 360 degree safe framework. The framework can be found at:

http://www.360degreesafe.org.uk