E-safety policy

Reviewed: September 2017

Contents Page

Responsibilities

The members of SLT team responsible for e-safety is	Jo Watson
The governor responsible for e-safety is	Louise Prockter
The e-safety co-ordinators are	Jo Watson

The e-Safety co-ordinators are 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 college community. They may also be required to deliver workshops for parents.

E-Safety Committee

The school safety committee is convened by the e-safety officer. It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, parents, pupils.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community will sign an Acceptable Use Policy that is appropriate to their age and role. 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. This can be found in appendix 2

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

The AUP will form part of the first lesson of ICT for each year group and will be regularly referred to in ICT lessons.

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. This form is completed when the children start at school and kept with their individual records.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

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

Staff should always use a school camera 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 only permitted to take photos/videos of their OWN children in school events. They are requested not to share any 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.

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 staff mobile phones should be kept locked away securely in the classrooms during the school day. At no time should staff use their phones in the classroom or around the pupils.

All pupil mobile phones should be kept in the basket in the Safeguarding Office and only collected upon leaving the school at the end of the day. Any pupil discovered using a mobile phone in school will have it removed and placed in the Safeguarding Office.

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 for 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 logon. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector 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 be used in school. Staff need to self risk assess any data that they plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact. However the operating system set up within school will minimise the use of USB pens as it can be logged onto at home to work on any information required and the use of USB pens will be phased out in time.

Reporting

All breaches of the e-safety policy need to be recorded in the ICT reporting book that is kept in the Safeguarding Office. 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 Lead immediately – it is their responsibility to decide on appropriate action not the class teachers.

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

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's LADO should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg Ceop button, trusted adult, Childline)

Infringements and sanctions

Whenever a student or staff member infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

(a) Students

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Use of unauthorised instant messaging / social networking sites

Sanctions: refer to class teacher / e-Safety Coordinator (To report to SLT)

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued use of unauthorised instant messaging / social networking sites
- 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

Sanctions: refer to Class teacher/ e-safety Coordinator (To report to SLT) / removal of Internet access rights for a session/ contact with parents

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

Sanctions: referred to Class teacher / e-safety Coordinator (To report to SLT) / Headteacher / removal of Internet rights for a period / contact with parents

Other safeguarding actions

If inappropriate web material is accessed:
Inform Designated Safeguarding Leads.
Ensure appropriate technical support filters the site

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

Sanctions – Refer to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer

Other safeguarding actions:
Secure and preserve any evidence
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 related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright or license e.g. installing unlicensed software on network

Sanction - Headteacher. Warning given.

Level 2 infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school 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 the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

Sanction – Headteacher / Governors and follow school disciplinary procedures; report to LA Personnel/ Human resources, report to Police.

Other safeguarding actions:

Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
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 the 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, 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 in social networking sites.
Staff must not post pictures of school events without the Headteacher's consent
Staff must not use social networking sites within school
Staff need to use social networking in a way that does not conflict with the GTC code of conduct , TDA Core Standards or Personnel handbook
Staff should review and adjust their privacy settings to give them the appropriate level of privacy

Staff communication

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

- Post on school letter headed paper
- School telephone system
- School e-mail system

The following are excluded from the official channels:

- Social networking sites
- Gaming sites

- Chatrooms
- Personal mobile phones
- Personal e-mail addresses
- Personal video conferencing solutions (eg Skype)

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 ICT 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 school 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) E-safety training is an integral part of Child Protection / Safeguarding
b) training and vice versa
c) An audit of e-safety training needs is carried out regularly and is
d) addressed
e) All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
f) 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
g) Staff are encouraged to undertake additional e-safety training, e.g. CEOP
h) The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
i) The school takes every opportunity to research and understand good practice that is taking place in other schools.
j) School will ensure that children are safe from terrorist and extremist material when accessing the internet in school by having secure filters which will block inappropriate content.

k) Pupils and staff are aware of the procedures in school for reporting any concerns relating to inappropriate content found on the internet.
l) Governors are offered the opportunity to undertake training.

Parents and the wider community

There are regular e-safety information sharing sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinator with input from the e-safety committee.

Monitoring and reporting

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

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

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

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

Signed: _____(Governor)
Date: Sept 2017
Next Review date: Sept 2018

Appendices

Appendix 1 – AUP's

AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- 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 mum, dad, carer or teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- in school only email people I know or if my teacher agrees
- in school only use my school email
- talk to my mum, dad, carer or teacher before using anything on the internet
- not tell people about myself online (I will not tell them my name, anything about my home, family or pets)
- not upload photographs of myself without asking a teacher or responsible adult
- never ever agree to meet a stranger

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

I am aware of the CEOP report button and know when to use it.

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 have been approved by my parent/carer or teacher
- work only with people my school has approved and will deny access to others
- respect the school security system for the computers, i-pads etc
- 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
- only give my mobile phone number to friends I know in real life and trust
- in school only email people I know or approved by my school
- in school only use email which has been provided by school
- discuss and agree my use of a social networking site with a responsible adult before joining
- 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
- never meet an online friend

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

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.

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 school network security
- implement the school's policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- 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 know that anything I share online may be monitored.

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.

Continued…

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
- 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 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 takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, 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

Appendix 2 – Parent letter – internet/e-mail use

Parent / guardian name:……..
Pupil name: …….
Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that in school they can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community. I will not upload any photographs of children wearing the school logo. If we discover that you have broken this agreement the right to take photos/videos will be removed.

Parent's signature:…… **Date:**…….

Appendix 3 – School audit

Audit

The self-audit in 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/No

Date of latest update (at least annual): _____

The Leadership team member responsible for e-safety is: _____

The governor responsible for e-Safety is: _____

The designated member of staff for child protection is: _____

The e-Safety Coordinator is: _____

The e-Safety Policy was approved by the Governors on _____

The policy is available for staff at: _____

The policy is available for parents/carers at: _____

Appendix 5 – Links

(a) Shropshire Council Advisory Service documentation

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

https://www.shropshirelg.net/esafety/staff/Pages/welcome.aspx

(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