Coleham Primary School

E-Safety Policy - Pupil Use of ICT

Policy Date: September 2016

AUTHOR TO

Contents Page

Responsibilities

The member of SLT team responsible for e-safety is: **Claire Jones**

The governors responsible for e-safety are: **Kevin Quigley & Greg Giani**

The e-safety co-ordinators are: **Lotte Heap & Katrina Harrison**

The e-Safety co-ordinators are responsible for 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 school community.

E-Safety Committee

E-Safety is governed under the Finance, Personnel, Premises and Health and Safety Committee. E-Safety matters are dealt with by the Subject Leaders for ICT and the ICT Development Working Group which invites representatives from SLT, the ICT Technician, the School Business Manager and Governors with ICT Special Interest.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community agree to an Acceptable Use Policy that is appropriate to their age and role. The AUPS used can be found in appendix 1 and also within the Information and ICT Security Policy.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip. This can be found in appendix 2.

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

The AUP will form part of the lesson plans for 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 and SRE. 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 needs 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 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.

A template Consent form is at appendix 4.

Staff should always use a school camera or school Ipads 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

Children in Years 5 and 6 are permitted to bring mobile phones to school subject to the terms and conditions of the Mobile Phone Agreement. Pupils' mobile phones should be switched off whilst on the school premises and their phones must be handed into their class teacher. Pupil phones found to contravene this should be confiscated by the class teacher and returned at the end of the school day.

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.

Use of e-mails

Pupils 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 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. Passwords must not be shared. 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 school owned memory sticks are to be used in school which should be signed out to members of staff by the ICT Technician.

Reporting

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

Incidents which may lead to child protection issues must be passed on to the Designated Safeguarding Lead or one of the Deputy Safeguarding 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 Safeguarding Lead or a Deputy Safeguarding 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 day.

Allegations involving staff should be reported to the Designated Safeguarding Lead or to a Deputy Safeguarding Lead and the Headteacher. If the allegation is one of abuse then it should be handled according to the school policy 'Dealing with Allegations of Abuse against Staff'. Where it is the Headteacher who is the subject of the allegation or concern, the member of staff should discuss the matter with the most senior Designated Teacher or with the next most senior available member of staff.

If necessary the Local Authority's Designated Officer 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 pupil 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:

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 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 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 / 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.

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.

Social networking

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

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). 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 school 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). Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
g). The culture of the school 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

There is a planned programme of e-safety sessions for parents, carers, etc. This is planned, monitored and reviewed by the e-safety co-ordinators.

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, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

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

- the school'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.

Appendix 1-

Coleham Primary School Information & Communication Technology (ICT)

Acceptable Use Agreement for learners in KS1

I want to feel safe all the time at school.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only communicate with people I know in real life, not people I don't know online
- 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
- not give my mobile phone number to anyone who is not a friend in real life
- check with my teacher before using 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

I understand that anything I do on the computer may be seen by someone else.

Name of pupil:_____

Class: _____

Signed (Parent or guardian):_____

Print name (Parent or guardian):_____

Date: _____

Coleham Primary School Information & Communication Technology (ICT)

Acceptable Use Agreement for learners in KS2.

When I am using the computer or other technology at school, I want to feel safe.

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 to my work at the time
- 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 strangers or any message that seems offensive or unpleasant and report it straight away to my teacher
- 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 time, only email people I know or who are approved by my school
- only use email in school time which has been provided by school, as part of a lesson
- 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
- talk to a responsible adult if a friend I've met online wants to meet me. Never arrange to meet an online friend by myself.

- **I know that teachers will have access to anything I produce using ICT in school.**
- ***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.***

Name of pupil:_____

Class:_____

Signed (Parent or guardian):_____

Print name (Parent or guardian):_____

Date: _____

Coleham Primary School Information & Communication Technology (ICT)

Acceptable Use Policy for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to support 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 a Senior Information Risk Oficer (SIRO)
- an Information and ICT Security policy has been written by the school.
- the ICT Security policy and its implementation will be scheduled for review regularly
- 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
- 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

Signed:

Date:

Print name:

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, 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 the school 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

Parent's signature:…….
Date:…….

Appendix 3 – School 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):
_____

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:
_____

Date of E-safety training for staff
_____

Date of Prevent training
_____

Appendix 4 – Photo/video consent

School Name:

Name of child:

Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.

To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please give the completed form to the school office. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child's image in our printed promotional publications?
   Yes / No

2. May we use your child's image on the school website/SLG?
   Yes / No

3. May we record your child's image on our promotional videos?
   Yes / No

4. May we use your child's image in the local press?
   Yes / No

Signature: Date:

Your name (in block capitals):

Appendix 5 – 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

Appendix 6

Shropshire Council has developed an e-safety policy for school staff which has been agreed by the following Professional Associations / Trade Unions representing staff in schools:-

- National Union of Teachers
- National Association of Schoolmasters Union of Women Teachers
- Association of Teachers and Lecturers
- National Association of Head Teachers
- Association of School and College Leaders
- UNISON
- GMB

The policy can be found at:

https://www.shropshirelg.net/services/hr/noticeboardnews/Documents/E-Safety%20Policy.pdf