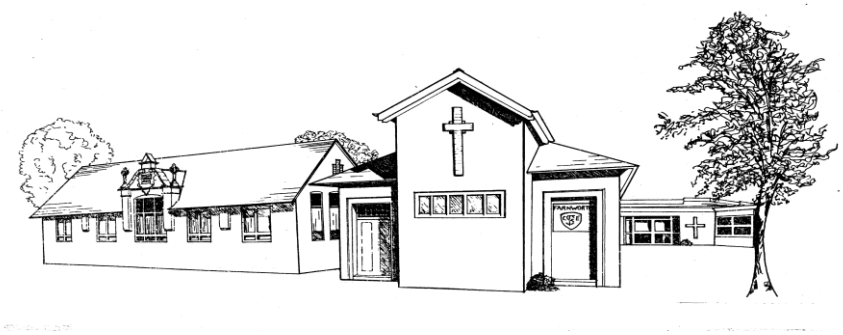


FARNWORTH CHURCH OF ENGLAND PRIMARY SCHOOL

e-Safety Policy

Recommended by	H Whitfield
Originally approved by	Finance, Premises, Health, Safety and Welfare Committee
Original approval date	17.10.12
Current version number	3.4
Current version approved by	Finance, Premises, Health, Safety and Welfare Committee
Current version approval date	19.10.15
Current version review date	This is a live policy and, as such, is kept under constant review to reflect changes in legislation and impact assessments. Formal review date: **Jan 2020**

CHANGE RECORD FORM

Version	Date of change	Date of release	Changed by	Reason for change
2.1	September 2012	October 2012	C.Crank	Policy review
3.1	September 2014	25.9.14	C.Crank / J. Stillings	Policy review
3.2	October 2015	19.10.15	J. Stillings / L. Le Marinel	Policy review
3.3	October 2016	Oct 2016	J. Stillings / L. Le Marinel	Policy review
3.4	January 2018		L Le Marinel	Adopt LA Model policy
3.5	Oct 2018	9.10.18	J. Stillings	Change to personnel
3.6	January 2019	4.3.19	H. Whitfield	Policy review

CONTENTS **Page**

1. **Responsibilities** **5**
2. **Internet Use and acceptable Use Policies (AUPS)** **6**
3. **The Prevent Duty** **6**
4. **Photographs and Video** **7**
5. **Mobile Phones and other Devices** **8**
6. **Use of e-mails** **9**
7. **Security and Passwords** **9**
8. **ICT Technical Support Staff** **9**
9. **Data Storage** **10**
10. **Reporting** **10**
11. **Infringements and Sanctions** **10**
12. **Rewards** **11**
13. **Social Networking** **12**
14. **e-Safety Education** **12**
15. **Parents and the Wider Community** **12**
16. **Monitoring and Reporting** **13**
17. **Equal Opportunities** **13**
18. **Review Procedure** **13**

Appendices **Page**

Appendix 1 - Acceptable Use Policies **15 - 19**

Appendix 2 – Parent Letter **20**

Appendix 3 – School Audit **21**

Appendix 4 – Photo/Video Consent **22**

Appendix 5 – e-Safety Incident Log **23**

Appendix 6 – Responding to incidents of misuse – flow chart **24**

Appendix 7 – Record of Reviewing Services/Internet Sites **25**

Appendix 8 - Legislation **26 - 29**

Related Policies:

This policy is part of a whole school strategy to ensure that all members of our school community are kept safe and that their welfare is a high priority. It should be read in conjunction with the following policies:

Policies	
• Allegations Against Adults • Attendance and Pupil Leave of Absence • Children Missing Education • Confidentiality • Emergency planning • Equalities • Good Behaviour and Anti-bullying • Intimate Care • Policy for children missing education • Safeguarding • Safer Recruitment	• Sex and Relationships Education • Social Media • Staff Behaviour / Code of Conduct • Special Educational Needs and Disability • Supporting Children with Medical Conditions in School • Use of Physical Intervention / Restraint • Whistleblowing • Working with separated families

SCOPE

In the interests of pupil safety, the school maintains a zero tolerance attitude to the misuse of electronic media, including bullying, in any form and maintains high expectations in keeping everyone safe. We recognise the need to discuss aspects of e-Safety by maintaining its high profile. This policy relates to the aspects of setting out our zero tolerance approach, having high expectations of all users, and managing incidents of reported misuse.

This policy applies equally to all pupils, staff, Governors and visitors to the school.

AUTHORITY

We wish to ensure that every child remains safe at Farnworth CE Primary School, whilst striving for the highest possible standards of pupil engagement. Farnworth CE Primary School recognises the importance of e-Safety management and gives the highest importance to the safeguarding and welfare of children.

Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism" (Prevent Duty Guidance, *HM Government* 2015). All members of staff must have regard to this guidance when carrying out that duty.

STATEMENT OF POLICY

ICT in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Farnworth CE Primary School is committed to building in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Virtual Learning Platforms
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Forums, Wikis and Blogs
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile / Smart phones with text, video and / or web functionality
- Other mobile devices with web functionality

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

We understand the responsibility to educate our pupils on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, Governors, visitors and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc); and technologies owned by pupils and staff, but brought onto school premises utilising the school's network (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc).

We will educate our pupils to prevent them from being drawn into terrorism and radicalisation, teaching them of the risks that are present, and ensuring that they are given appropriate advice and support. We want Farnworth CE Primary School to be a safe space in which children and young people can understand and discuss sensitive topics, including terrorism and the extremist ideas that are part of terrorist ideology, and learn how to challenge these ideas. We will ensure children are safe from terrorist and extremist material when accessing the internet in school, including by having established appropriate levels of filtering through the Local Authority.

1. Responsibilities

The Governors, with the advice of the Headteacher**,** have the overall responsibility to ensure that the policy and practices are embedded and monitored. All Governors should have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

The Headteacher has the overall responsibility to ensure that the policy and practices are embedded and monitored regularly. The Headteacher will be the designated Single Point Of Contact (SPOC) and must undertake Prevent training in fulfilling their duties.

The e-Safety Coordinator in this school, as a designated member of the Senior Leadership Team, is Mrs Whitfield. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as Halton LA, CEOP (Child Exploitation and Online Protection) and Childnet, and to up-date all staff. The e-Safety co-ordinator will also organise workshops and information sessions for parents/carers to attend.

The e-Safety Coordinator is responsible for ensuring the web filtering system is at a minimum acceptable level and report any concerns to the SPOC.

The Subject Leader has responsibility for ensuring all staff have received appropriate and relevant training to sufficiently deliver this policy.

All Staff are responsible for their own actions under the Acceptable Use Agreement and in keeping with the Staff Code of Conduct. Staff must immediately report any incident which breaches e-Safety, **in particular under the Prevent Duty**, to the e-Safety Coordinator.

All staff are responsible for identifying children who may be vulnerable to radicalisation and must follow these steps:

- assess the risk of children being drawn into terrorism, including support for extremist ideas that are part of terrorist ideology;
- keep children safe from terrorist and extremist material when accessing the internet in school, which includes educating children how to safe online;
- provide a safe environment which embeds British Values within the curriculum building resilience to radicalisation and encouraging debate that helps children understand how to influence and participate in decision making.

If you have any concerns you should immediately inform the ***Single Point of Contact person (the Headteacher).***

ADDITIONAL GUIDANCE

e-Safety skills development for staff

- Our staff receive regular information and training on e-Safety issues in the form of regular staff training.
- New staff receive information on the school's acceptable use policy as part of their induction.
- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community.

- All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the school e-Safety messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and / or related technologies are used.
- The e-Safety policy will be introduced to the pupils at the start of each school year.
- e-Safety posters will be prominently displayed in classrooms and around school.

e-Safety in the Curriculum

- Educating pupils on the dangers of technologies that may be encountered outside school is done informally when opportunities arise and as part of the e-Safety curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent /carer, teacher/trusted staff member, or an organisation such as Childline / CEOP report abuse button.

2. Internet use and Acceptable Use Policies (AUPs)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. An example of our school's AUPS can be found in appendix 1. A copy of the pupil AUP will be sent to parents with a covering letter/reply slip at the start of each new academic year. This can be found in appendix 2.

AUP's will be reviewed annually. All AUPs will be stored centrally in case of breaches of the e-Safety policy. The AUP will form part of the first lesson of the computing curriculum for each year group.

3. The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and Security Act 2015 on specified authorities (including 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 computing 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 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

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

4. 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/carers 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. This is updated annually as part of the data collection exercise.

Staff should always use a school camera or i-pad to capture images and **should not** use their personal devices.

Photos taken by the school are subject to the GDPR.

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.

Parents attending school based events will be reminded of their responsibilities in relation to social media verbally and through notices.

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 GDPR

5. Mobile phones and other devices

Farnworth CE Primary recognises that staff may need to have access to mobile phones on site during the working day. However, there have been a number of queries raised within the local authority and nationally regarding the use of mobile phones and other devices in educational settings.

The concerns are mainly based around these issues:

- Staff being distracted from their work with children
- The use of mobile phones around children
- The inappropriate use of mobile phones

Ensuring the Safe and Appropriate Use of Mobile Phones

Farnworth CE Primary School allows staff to bring in mobile phones for their own personal use. However, they must be kept securely at all times and are not allowed to be used in the toilets, changing areas or in the play areas at any time. If staff fail to follow this guidance, disciplinary action will be taken in accordance to the school's staff code of conduct. If staff need to make an emergency call, they must do so either in the main or Headteacher's office. Staff must ensure that there is no inappropriate or illegal content on the device.

Mobile phone technology may not be used to take photographs anywhere within the school grounds. There are digital cameras and tablets available within the school and only these should be used to record visual information within the consent criteria guidelines of the local authority and the school.

Members of staff may only contact a parent/carer on school approved mobile phones. With the exception of Year 6, pupils should not use mobile phones within the school grounds and should not bring in a mobile to school at any time. Year 6 are allowed to do this only when parental written consent has been given.

Use of Mobile Phones for Volunteers and Visitors

Upon their initial visit volunteers and visitors are given information informing them they are not permitted to use mobile phones when in proximity to the children.

If volunteers and visitors wish to make or take an emergency call they may use either the main or, with their permission, the Headteacher's office. Neither are volunteers or visitors permitted to take photographs or recordings of the children without the Headteacher's permission.

We believe that photographs validate children's experiences and achievements and are a valuable way of recording milestones in a child's life. Parental permission for the different ways in which we use photographs is gained as part of the initial registration at this school. We take a mixture of photos that reflect the pre-school environment; sometimes this will be when children are engrossed in an activity either on their own or with their peers. Children are encouraged to use the i-pad to take photos of their peers. In order to safeguard children and adults and to maintain privacy, cameras are not to be taken into the toilets by adults or children. All adults whether teachers/support staff or volunteers at the school understand the difference between appropriate and inappropriate sharing of images.

All images are kept securely in compliance with the GDPR.

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 or the Designated Safeguarding Lead who will deal the matter in line with normal school procedures. It should be noted that it is a criminal offence to use a mobile phone to menace, harass or offend another person. In such circumstances the school may consider it appropriate to involve the police.

Use of Mobile Phones for Children

Children are not allowed to bring mobile phones to school unless in Year 6. Year 6 children will only be allowed to bring in a mobile phone with written permission from their parent/carer with regards to walking home. There are no reasons why a child needs to use or have in their possession, a mobile phone during the school day. Parents/carers are reminded that in cases of emergency the school office remains a vital and appropriate point of contact and can ensure your child is reached quickly and assisted in any appropriate way.

In exceptional circumstances the school may allow a child's mobile phone onto the school premises. This will only take place after the parent/carer have previously sought approval from the Head Teacher. In this instance the mobile phone will be given to the class teacher and securely stored until the end of the day. The mobile phone must remain switched off whilst in school. If a child brings a mobile phone to school without prior arrangement with the Head Teacher the phone will be removed from the pupil for safekeeping. The phone will be stored safely in the school office and the parent/carer will have to collect the mobile at the end of the school day. **NB This is a change to policy and takes effect Monday 22 January 2018.**

6. 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.

7. Security and passwords

Passwords should be changed regularly. Passwords **must not** be shared. Staff must always 'lock' their classroom 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.

8. ICT Technical Support Staff

The school uses AppleCore for its technical support. The lCT Systems Manager, Paul Kennedy is responsible for ensuring that:

- The IT technical infrastructure is secure:
  - i. Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
  - ii. Windows updates are regularly monitored and devices updated as appropriate.
  - iii. Any e-safety technical solutions such as Internet filtering are operating correctly.

iv. Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the e-safety officer and Headteacher.
v. Passwords are applied correctly to all users regardless of age

9. Data storage

Only encrypted USB pens should be used in school.

10. Reporting

All breaches of the e-safety policy need to be recorded in the Computing 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 need to be passed on to the Designated Safeguarding Lead (Mrs Whitfield) immediately – it is her responsibility to decide on appropriate action not the class teacher's.

Incidents that are of a concern under the Prevent duty should be referred to the Designated 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 intervention (e.g. cyberbullying) should be reported to Mrs Stillings or Mrs Whitfield on 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 (e.g. CEOP button, trusted adult, ChildLine).

11. Infringements and sanctions

Whenever a child 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
- 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
- Unauthorised use of mobile phone (or other new technologies)
- Continued use of unauthorised instant messaging / social networking sites
- Use of File sharing 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 GDPR.
- 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.

12. 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 – e.g. class reward system

(house points) for good research skills, certificates for being good cyber citizens etc. The E-safety co-ordinator will indicate these opportunities.

13. Social networking

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

14. e-Safety 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). Regular 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 officers, 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). 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
d). 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
e). Staff are encouraged to undertake additional e-Safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) e-Safety Certificate
f). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
g). The school takes every opportunity to research and understand good practice that is taking place in other schools
h). Governors are offered the opportunity to undertake training.

15. Parents/Carers 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-ordinator.

16. 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, pupils, parents / carers
c). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Halton Local Authority (where necessary)
- Halton Safeguarding Children Board

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

17. Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents/carers for all pupils and this in turn should aid establishment and future development of the schools' e-Safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children.

18. Review Procedure

The e-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place or if Central Government change the orders or guidance in any way. (See Appendix 5 Current Legislation). The next anticipated review date will be: **January 2020.**

Appendices

Appendix 1 – Acceptable Use Policies

Acceptable Use Policy 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 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 CEOP report button and can ask a trusted adult when to use it.

Signed (child) NB Year 2 only:……

Signed (parent): FS and Y1: ……..

Acceptable Use Policy 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
- obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- 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

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 (child):_____

Acceptable Use Policy 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 (e.g. 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.

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

- 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.
- forward chain letters

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 _____

Your name (in block capitals): ……

Date:…….

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 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 an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school
- 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

FARNWORTH CE PRIMARY SCHOOL

Parent / guardian name:……..

Child's name: …….

Child's 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 (via e-schools) 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 school 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 / Guardians' signature:……

Your name (in block capitals): ……

Date:…….

Appendix 3 – School 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 Halton guidance? **Yes**/No

Date of latest update (at least annual): **February 2019**

The Leadership team members responsible for e-safety are: **Mrs Stillings & Mrs Whitfield**

The governor responsible for e-Safety is: **Mr Keith McKnight.**

The designated member of staff for child protection is: **Mrs Whitfield**

The e-Safety Coordinator is: **Mrs Whitfield**

The policy is available for staff at: **School website and staffroom folder**

The policy is available for parents/carers at:
eSafety policy

Date of E-safety training for staff: **CEOP 2017 delivered by PC Jane Tetlow**.

Date of Prevent training: **05/09/16**

Appendix 4 – Photo/video consent

FARNWORTH CE PRIMARY

Name of pupil: _____

Class: _____

During the year the staff may 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. 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? 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:……..

Your name (in block capitals)…….

Date: ……..:

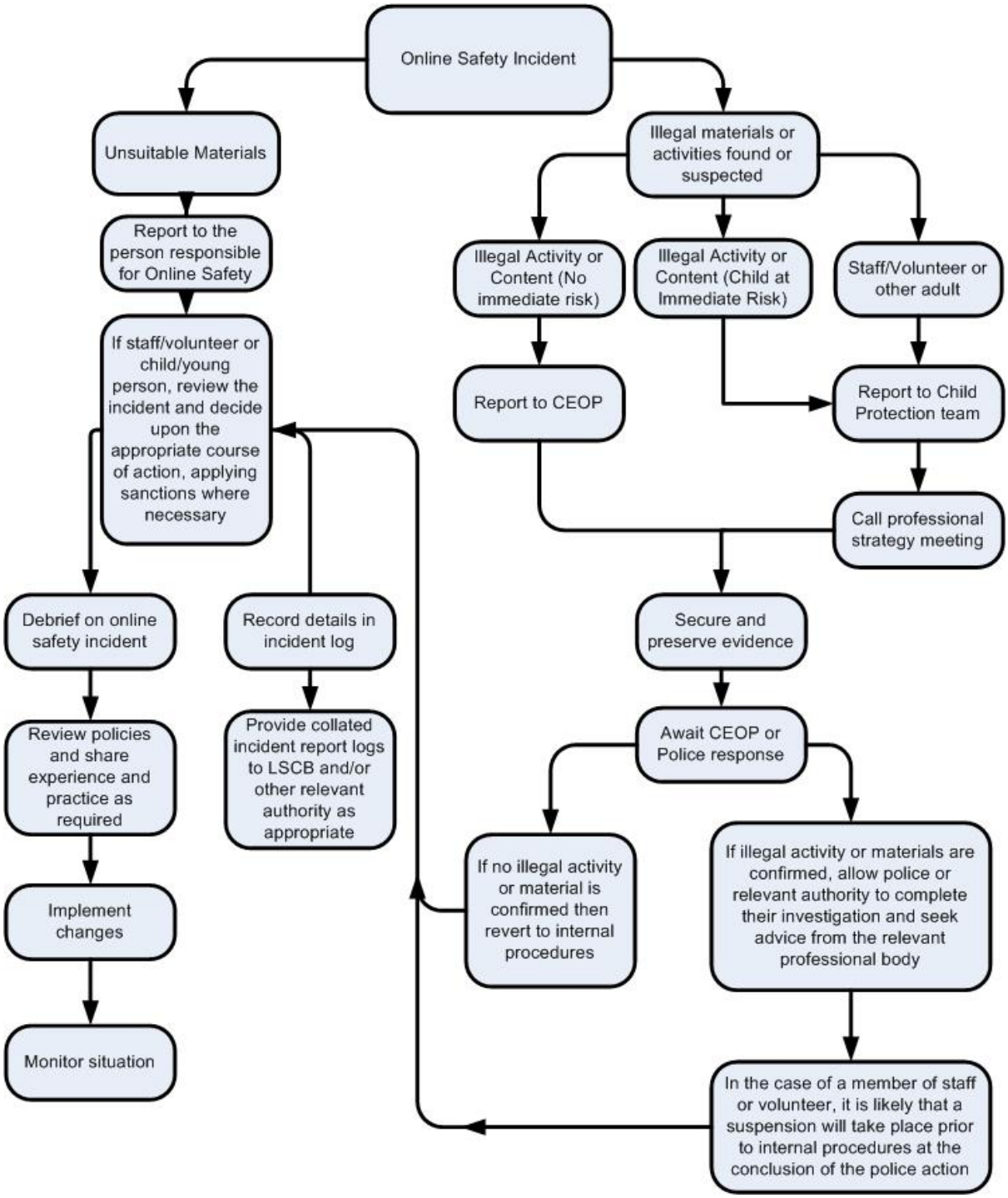
Appendix 5

Farnworth CE Primary School - e-safety incident log

e-Safety Incident Log Details of ALL e-Safety incidents to be recorded by the e-Safety Coordinator.						
Date	Time	Details of Incident (including evidence and / room / computer / device number)	Action taken		Incident Reported by	Signature
			What?	By whom?		

Appendix 6

Responding to Incidents of Misuse – flow chart



Appendix 7

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device Reason for concern

Conclusion and Action proposed or taken

Appendix 8

Legislation

Schools should be aware of the legislative framework under which this E-Safety Policy has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- "Eavesdrop" on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual's data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. YouTube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or
- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (DfE guidance – http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation

The Protection of Freedoms Act 2012

Requires schools to seek permission from a parent / carer to use Biometric systems

The School Information Regulations 2012

Requires schools to publish certain information on its website:
http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations