Farmor's School
AN ACADEMY

E-SAFETY POLICY

Author:	**Noelle Sturla**
Date of approval:	**17th April 2018**
Next Review date:	**April 2021**
Review period:	**3 years**
Status:	**Recommended**

1. PURPOSE

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. Our school E-Safety policy helps to ensure safe and appropriate use of ICT by all members of our school community, at all times. This policy has been developed in accordance with the statutory guidance 'Keeping Children Safe in Education' (DfE 2016) and the Prevent Duty (Counter Terrorism and Security Act, 2015)

2. RELATIONSHIP TO OTHER POLICIES

2.1 This policy is linked to, and should be read in conjunction with, the following school policies and procedures:

- Internet Acceptable Use Policies (staff and pupils)
- Safeguarding Children Policy
- Behaviour and Exclusion Policy
- Code of Conduct (for Adults)
- Conduct Policy
- Allegations of Abuse by Staff Policy
- Anti-bullying Policy
- Health & Safety Policy

3. SCOPE, PRINCIPLES AND DEFINITIONS

3.1 This policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents, carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

3.2 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school.

3.3 The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place, whether in or out of school.

4. ROLES AND RESPONSIBILITIES

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

4.1 Governors

4.1.1 Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the Safeguarding Strategy Group (comprised of the Headteacher, School Business Lead, Designated Safeguarding Lead, PSHCE Lead Teacher and representative Governors) who will receive an annual report about e-safety incidents.

4.1.2 The outcomes of this review will be reported to the Governing Board by their representative on this group.

4.2 The Headteacher and Senior Leadership Team responsibilities

4.2.2 The Headteacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the Network Manager and Senior Leaders.

4.2.3 The Headteacher and other relevant Senior Leaders are responsible for ensuring that the relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as necessary.

4.2.4 The Headteacher and other relevant Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

4.2.5 The Headteacher and Senior Leaders should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff (see Conduct Policy and Allegations of Abuse by Staff Policy).

4.3 The Designated Safeguarding Lead responsibilities

The Designated Safeguarding Lead will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with the other Senior Leaders over specific incidents
- liaise with the Network Manager to ensure that filtering is effective in safeguarding children
- regularly monitor filtering
- receive reports of e-safety incidents and monitor actions taken by staff
- meet regularly with Governors to discuss current issues, review incident logs and filtering
- be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from: sharing of personal data; access to illegal and/or inappropriate materials; inappropriate on-line contact with adults and/or strangers; potential or actual incidents of grooming; cyber-bullying

4.4 The Network Manager and ICT Support staff responsibilities

The Network Manager and ICT Support staff will take reasonable measures to ensure:

- that the school's ICT infrastructure is secure and is protected against misuse or malicious attack
- the school's internet connection provider is informed of issues relating to filtering
- the school's filtering system is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person

- that they are up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network and email is regularly monitored in order that any misuse or attempted misuse can be reported to the Headteacher or other relevant Senior Leader for investigation and appropriate actions and sanctions
- that monitoring software and systems are implemented and updated in line with the policies of the supplying organisations.
- that all data is wiped or overwritten as appropriate from any equipment before disposal

4.5 The Teaching and Support Staff responsibilities

Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school E-Safety Policy and practices
- they have read, understood and signed the school Staff Acceptable Use Policy (Appendix A)
- they report any suspected misuse or problem to the Headteacher or relevant member of the Senior Leadership Team for investigation and appropriate action
- e-safety issues are embedded in the curriculum, where relevant, and other school activities
- they monitor ICT activity in lessons, extra-curricular and extended school activities
- in lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material found in internet searches
- they follow the agreed process for dealing with a sexting incident (Appendix C).

4.6 Pupil responsibilities

Pupils:

- are responsible for using the school ICT systems in accordance with the pupil Acceptable Use Policy, which they will be expected to sign before being given access to school systems
- must have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand-held devices
- must understand that they must not access inappropriate material using the school's computer systems at any time or using their own equipment ('phone, tablet, laptop etc.) on the school site, during the school day or when engaged in any school activity.

4.7 Parents and Carers

Parents and other carers play a crucial role in ensuring that their children understand the need to use computers and mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues. Parents and carers will be made aware that their child/children have signed the pupil Acceptable Use Policy and will be able to access a copy. Information and updates will be made available on the school website and through weekly parent bulletins.

5. E-SAFETY EDUCATION

5.1 Pupils

Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience. E-Safety education will be provided in the following ways:

- In Year 7, all pupils receive a series of lessons focussing on e-safety.
- All Year 7 pupils receive a copy of the Student Internet Acceptable Use Policy agreement in their induction pack. The pupils and parents/carers sign the agreement which is then returned to school.
- The Pupil Internet Acceptable Use Policy agreements are read by all pupils and agreed to annually.
- A planned e-safety programme is provided as part of the IT and PHSCE programmes and is regularly revisited – this covers the use of computing and new technologies both in school and outside school.
- Key e-safety messages are reinforced as part of a planned programme of assemblies and tutorial activities.
- Pupils are taught to be critically aware of the materials and content they access on-line and are guided to consider the accuracy of information.
- Pupils are helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff act as good role models in their use of ICT, the internet and mobile devices.

5.2 Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy.

- All staff have to sign the Staff Internet Acceptable Use Policy agreement as part of the annual statutory information they are required to read
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policies

- The Safeguarding Strategy group will receive regular updates through attendance at relevant training sessions and by reviewing guidance documents released by DfE and other relevant bodies
- Updates to the E-Safety Policy and guidelines will be brought to the attention of all members of staff as and when necessary
- Staff awareness of e-safety will be maintained by an item on the agenda for one of the staff meetings at the start of each academic year
- The Designated Safeguarding Lead and Network Manager will provide advice, guidance and training as required to individuals as required

5.3 Governors

Governors should take part in e-safety training/awareness sessions, with particular importance for those who are members of any sub-committee or group involved in computing, ICT, e-safety, health and safety or safeguarding.

6. TECHNICAL – INFRASTRUCTURE/EQUIPMENT, FILTERING AND MONITORING

The school will be responsible for ensuring that the school's network infrastructure is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems by the Designated Safeguarding Lead and Network Manager.
- Servers, wireless systems and cabling must be located as securely as possible and physical access restricted.
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Network Manager's Line Manager.
- All users will be provided with a username and password by the school network manager who will keep an up to date record of users and their usernames.
- The administrator passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Headteacher or School Business Lead and kept in a secure place (e.g. school safe).
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by the school's internet connection provider.
- In the event of the Network Manager (or other person) needing to switch off the filtering for any reason, or for any user, this must be agreed with the Headteacher or Designated Safeguarding Lead in advance and the details of the reason and the duration of the unfiltered access logged.
- Any filtering issues should be reported immediately to the school's internet connection provider by the Network Manager.
- Requests from staff for sites to be removed from the filtered list will be considered by the Network Manager and referred to the Designated Safeguarding Lead.

- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Users must report any actual or potential e-safety incident to the Network Manager (or other relevant person).
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, visitors) onto the school system.
- The school infrastructure and individual workstations are protected by up to date virus software. Personal data should not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

7. UNSUITABLE AND INAPPROPRIATE ACTIVITIES

7.1 Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination or promotion of racial or religious hatred
- threatening behaviour, including promotion of physical violence or mental harm
- any other information which breaches the integrity of the ethos of the school or brings the school into disrepute.

7.2 The school filtering software is set up to restrict and detect the activities listed in 7.1. We are compliant with the Prevent Duty (2015) which states that schools are required to ensure children are safe from terrorist and extremist materials when accessing the internet in school, including by establishing appropriate levels of filtering.

7.3 There may be times when infringements of the policy could take place, through careless, irresponsible or deliberate misuse. The response to any apparent or actual incident of misuse is detailed in the Conduct Policy. The processes in that policy will be followed.

8. CONSULTATION

Consultation in developing this policy has been carried out with the Network Manager and Safeguarding Strategy Group (including representative Governors)

9. MONITORING, REPORTING AND EVALUATION

9.1 The implementation of this policy will be monitored by the Designated Safeguarding Lead, Network Manager and the Safeguarding Strategy Group.

9.2.1 This policy will be reviewed every three years by the Policy Committee on behalf of the Governing Board.

9.3 Should a serious e-safety incident take place, the following people will be informed, as appropriate:

i. The school's designated safeguarding lead/Network Manager
iii. The Headteacher
iv. The Governor with responsibility for safeguarding
v. The Chair of Governors
vi. The Local Authority Designated Officer for Child Protection
vii. The police

9.4 The school will monitor the impact of the policy using:

i. Logs of reported incidents;
ii. Logs of internet activity (including sites visited);
iii. Internal monitoring data for network activity;
iv. Surveys of
    - pupils
    - parents/carers
    - staff

Appendix A

ACCEPTABLE USE POLICY (Staff)

ICT Acceptable Use Policy

Farmor's School is committed to providing ICT facilities (including internet, email and Office 365) to employees and to promoting employee awareness of the benefits and dangers involved. Improper use of the internet or email could bring the school into disrepute and may lead to legal claims against individuals and the school. Infringement of this policy by employees may be regarded as a disciplinary offence and in serious cases, may result in dismissal.

A copy of this policy is displayed around the school and is available on SharePoint.

Computer network

Obtaining, downloading, sending, printing, displaying, distributing or otherwise transmitting or gaining access to materials which are pornographic, obscene, discriminatory, unlawful, abusive, offensive or inappropriate will be regarded as gross misconduct and will lead to disciplinary action.

Distributing abusive, discriminatory or defamatory statements will be regarded as gross misconduct and will lead to disciplinary action.

You are responsible for the security of your passwords.
The network must not be used for commercial purposes, e.g. buying or selling goods.
The installation of software on the network must only be done with the approval of the Network Manager.
Any software that is installed must be covered by the appropriate licensing agreements.
Copyright of materials available on the network must be respected.

Internet / Email

Use of the Internet and email must be solely for educational purposes.
Use of the internet and email are subject to scrutiny by the school. Any action that might damage the good reputation of the school will be dealt with as a serious act of misconduct and will lead to disciplinary action.
Use of the internet for personal financial gain, gambling, political purposes or advertising is forbidden.
Emails sent from the school account should contain the same professional levels of language and content as applied to letters or other media.
You are responsible for the email you send and for any contacts you make that might result in inappropriate emails being received.
Posting anonymous messages and forwarding chain letters is forbidden.
Appropriate security must be used or applied before confidential or sensitive information is sent via the internet or email.

If you are in any doubt about any of the above, please seek advice.

Appendix B

ACCEPTABLE USE POLICY (Pupils)

ICT Acceptable Use Policy

Farmor's School is committed to providing ICT facilities (including internet, email and Office 365) to pupils and to promoting pupil awareness of the benefits and dangers involved. Infringement by pupils may result in the withdrawal of access to hardware or software and in serious cases (particularly those that break the law) pupils may be excluded and referred to the police. Improper use of the internet or email could bring the school into disrepute and may lead to legal claims against individuals and the school.

Computer network

You must not install, or attempt to install, programs of any type on a machine, or store programs on the computers or network, without permission.
You must not damage, disable or otherwise harm the operation of computers, or intentionally waste ICT resources.
You will not use the network for commercial purposes, e.g. buying or selling goods.
You must not disclose your password or use passwords intended for the use of others.
You must not use the network in a way that may harass, harm, offend or insult others.
You are expected to respect and not attempt to bypass security in place on the network.
You must not access, copy, remove or otherwise alter other people's work, or attempt to alter the settings on the computers.
You may not plug any personal device into the mains power, or into any school device e.g. via USB, either to use it or to charge it.

Internet / Email

You may access the internet only for study purposes or school authorised activities.
You must not use the internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive.
You are expected to respect the work and ownership rights of people outside school as well as pupils and staff. This includes abiding by copyright laws.
You must not engage in chat activities over the internet whilst at school.
You should be aware that messaging services available outside of school are open forums and subject to public scrutiny. Any incidents of abuse, discriminatory or defamatory statements or anything that might damage the good reputation of the school will be dealt with as serious acts of misconduct and will follow the same e-safety procedures as outlined on the reverse.
You will not give personal information such as your address or telephone number to those who you contact through use of the school's ICT systems.

Sanctions

Violations of these rules will result in the withdrawal of access to all ICT resources and a letter will be sent home to your parents/ guardian explaining the reasons for withdrawal.
Additional action may be taken by the school following the procedures outlined on the reverse.

Serious violations will result in the police being involved and / or other legal action taken.

Appendix C

Sexting: how to respond to an incident
An overview for all teaching and non-teaching staff in schools and colleges

This document provides a brief overview for frontline staff of how to respond to incidents involving 'sexting'.

All such incidents should be reported to the Designated Safeguarding Lead (DSL) and managed in line with your school's safeguarding policies.

The DSL should be familiar with the full 2016 guidance from the UK Council for Child Internet Safety (UKCCIS), ***Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People,*** (https://www.safeguardinginschools.co.uk/wp-content/uploads/2016/08/Sexting-in-schools-and-colleges-UKCCIS-August-2016.pdf) and should not refer to this document instead of the full guidance.

What is 'sexting'?

In the latest advice for schools and colleges (UKCCIS, 2016), sexting is defined as **the production and/or sharing of sexual photos and videos of and by young people who are under the age of 18**. It includes nude or nearly nude images and/or sexual acts. It is also referred to as 'youth produced sexual imagery'.

'Sexting' does not include the sharing of sexual photos and videos of under-18 year olds with or by adults. This is a form of child sexual abuse and must be referred to the police.

What to do if an incident involving 'sexting' comes to your attention

Report it to your Designated Safeguarding Lead (DSL) immediately.

- **Never** view, download or share the imagery yourself, or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL.
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL.

If a 'sexting' incident comes to your attention, report it to your DSL. Your school's safeguarding policies outline the codes of practice to be followed.

For further information

Download the full guidance Sexting in Schools and Colleges: Responding to Incidents and Safeguarding Young People (UKCCIS, 2016) at www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis