Fir Vale School E-Safety Policy and Procedures

September 2021

Date ratified:	9 December 2021
Approved	Full Governors
Ratified	Full Governors
To be reviewed	Autumn 2022
E-safety Lead:	M KEMALI

Contents

INTRODUCTION

Purpose of policy

The E-safety policy and the Acceptable Use Agreement is for all school stakeholders; staff, pupils, governors, visitors and parents 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); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.)

The purpose of this policy is to establish the ground rules we have at Fir Vale Academy Trust for using ICT equipment, the Internet and any online technology.

Information Communication Technology (ICT) has established itself as an essential resource to support learning and teaching in school and at home, to raise educational standards, to promote student achievement as well as playing an important role in the everyday lives of children, young people and adults. It also supports the professional work of staff and enhances the school's management information and administration systems.

Requirements

At Fir Vale Academy Trust, we educate our pupils on e-safety issues (embedded in the curriculum / assemblies). The school provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the school intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe whilst using the Internet and other communication technologies for educational, personal and recreational use.

ICT covers a wide range of resources including; web-based and mobile learning. Whilst exciting and beneficial both in and out of the context of education, ICT, particularly web-based resources, need to be consistently policed. Children and young people should have an entitlement to safe Internet access at all times. The requirement to ensure that children and young people are able to use the Internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This e-safety policy will help to ensure safe and appropriate use. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Dangers

Some of the dangers pupils may face include:

- Unauthorised access to, loss of or sharing of personal information.
- The risk of being subject to grooming by those with whom they make contact on the Internet.
- Access to illegal, harmful or inappropriate images or other content
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers.
- Cyber-bullying
- Access to unsuitable video/Internet games
- An inability to evaluate the quality, accuracy and relevance of information on the Internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is read and used in conjunction with other school policies; specifically Behaviour, Anti-Bullying, Safeguarding/Child Protection, Use, Health and Safety and Data Protection (including procedures for CCTV).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision, to build pupils' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

All staff and pupils must agree to abide by the School ICT Acceptable Usage Policy prior to using any School ICT facilities, Appendix 1.

E-SAFETY POLICY

Roles and Responsibilities

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

1. Governors

The role of the Governors / Safeguarding Governor is to:

- Ensure that the school follows all current e-safety advice to keep children and staff safe
- Approve the e-safety policy and review its effectiveness
- Support the school in encouraging parents and the wider community to become engaged in e-safety activities
- Regular review with the E-Safety Co-ordinator (MKE) (including e-safety incident logs, filtering/change control logs etc.)

2. Headteacher

The Headteacher has overall responsibility for e-safety provision. The day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator (MKE).

The Headteacher will:

- Take overall responsibility for data and data security
- Ensure the school uses an approved, filtered internet service, which complies with current statutory requirements
- Ensure that the e-safety coordinator and other relevant staff receive suitable CPD to enable them to carry out their E-Safety roles and to train other colleagues
- 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
- Receive regular monitoring reports from the E-Safety coordinator
- Be aware of the procedures to be followed in the event of a serious e-safety incident or an allegation being made against a member of staff or volunteer

3. E-Safety Coordinator (MKE)

The E-Safety co-ordinator will:

- Monitor e-safety alerts using Smoothwall application
- Record all alerts to identify trends
- Report serious incidents to Safeguarding Team via CPOMS
- Ensure that filtration are set appropriately (MKE / RM)
- Take day-to-day responsibility for e-safety issues and take a lead role in establishing and reviewing the school e-safety procedures and documents
- Ensure that e-safety education is embedded across the curriculum
- Deliver an assembly to update staff and students on new procedures
- Promote an awareness and commitment to e-safeguarding throughout the school community
- Liaise with the school ICT technical staff

- Ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident or allegation against a member of staff or volunteer
- Communicate regularly with Safeguarding team, SLT and the safeguarding governor/committee to discuss current issues, review incident logs and filtering/change control logs
- Ensure that the e-safety log is kept up to date
- Facilitate training and advice for staff and others working in the school
- Be aware of emerging e-safety issues and legislation, and of the potential for serious child protection issues to arise from:
    - Sharing of personal data
    - Access to illegal/inappropriate materials
    - potential or actual incidents of grooming
    - cyberbullying and the use of social media
    - Inappropriate online contact with adults/strangers

4. RM/Technical staff

Network Managers/Systems Manager/ICT Technician will:

- Report any e-safety related issues to the E-Safety Co-ordinator
- Ensure that users may only access the school's networks through an authorised and properly enforced password protection policy
- Users password should be changed periodically
- Ensure that the school's ICT infrastructure is secure and is not open to misuse or malicious attack e.g. Keeping virus protection up to date
- That the school meets the e-safety technical requirements outlined in the school acceptable use policy and any relevant local authority e-safety policy & guidance
- The school's policy on web filtering, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person;
- Ensure that access controls/encryption exist to protect personal and sensitive information held on school-owned devices
- That they keep up to date with the school's e-safety policy and 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/virtual learning environment / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator / Headteacher / Senior Leader for Designated Safeguarding Lead or safeguarding team
- Ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster and in order to complement the business continuity process
- Ensure that documentation of the school's e-security and technical procedures are up-to-date
- Ensure that 5 Guest Logins Username are available to use by visitors and trackable by Smoothwall

5. Data Manager (MSH)

It is the responsibility of the Data Manager to ensure that;

- All data held on pupils on school office machines have appropriate access controls in place
- All data held on pupils on the Learning Platform is adequately protected and backed up

6. All Staff

It is the responsibility of all staff to:

- Read, understand and help promote the school's e-safety policy and guidance
- Read, understand and adhere to the Staff Acceptable Use Policy/Agreement –Appendix 1
- Be aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- Report any suspected misuse or problem to the e-safety coordinator
- Record e-safety incidents on CPOMS
- Maintain an awareness of current e-safety issues and guidance e.g. through CPD opportunities
- Model safe, responsible and professional behaviours in their own use of technology
- Ensure that any digital communications with pupils are on a professional level and only through school-based systems, never through personal mechanisms, e.g. e-mail, text, mobile phones or social media messaging or posts

Teachers must:

- Ensure that e-safety issues are embedded in all aspects of the curriculum and other school activities
- Monitor, supervise and guide pupils carefully when engaged in ICT activity in lessons, extra-curricular and extended school activities
- Ensure that pupils are fully aware of research skills and are made aware of legal issues relating to electronic content such as copyright laws (embedded in curriculum)
- Ensure that during lessons where internet is used pupils are guided to sites checked as suitable for their use and that processes are known and used when dealing with any unsuitable material that is found in internet searches
- Monitor students when online using provided software e.g. AB-Tutor

7. Pupils

Considering the age and level of understanding, the key responsibilities of pupils are to:

- Use the school ICT systems in accordance with the Pupil Acceptable Use Policy (AUP), which they and/or their parents will be expected to sign before being given access to school systems
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- Know and understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so (embedded in ICT curriculum)
- Know what action to take if they or someone they know feels worried or vulnerable when using online technology
- Know and understand school policy on the use of mobile phones, digital cameras and hand-held devices
- Know and understand school policy on the taking/use of images and on cyber-bullying
- Understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's e-safety policy covers their actions in and out of school when accessing and/or using the school system
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home
- Help the school in the creation/review of the E-safety Policy and procedures

8. Parents

The school will take every opportunity to help parents understand issues related to safety through parents' evenings, newsletters, letters, website and information about national/local e-safety campaigns/literature.

The key responsibilities for parents are to:

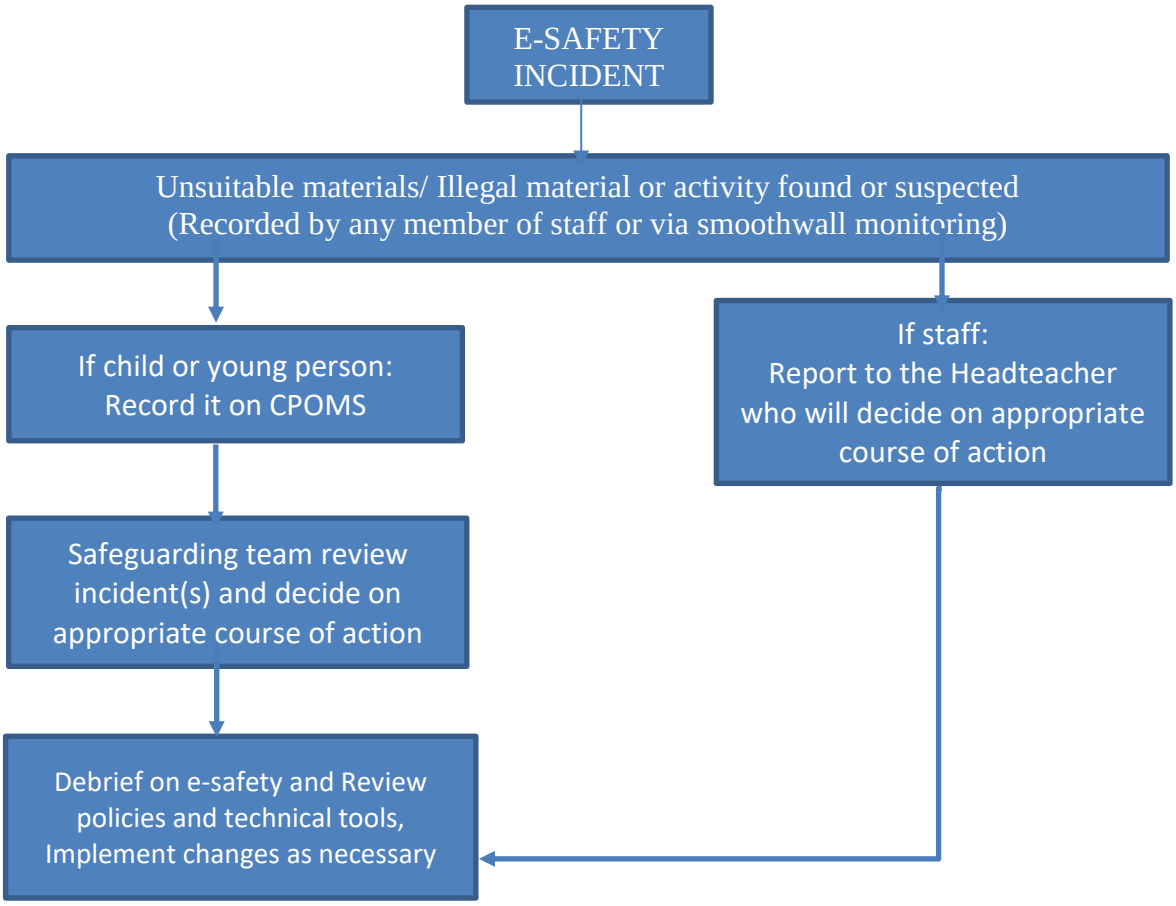
- Endorse the Pupil Acceptable Use Policy by which they and/or their child will be expected to sign before being given access to school systems
- Support the school in promoting e-safety which includes the pupils' use of the Internet and the school's use of photographic and video images
- Support the school in promoting e-safety which includes the pupils' use of the Internet and the school's use of photographic and video images
- Access the school website in accordance with the relevant school Acceptable Use Policy
- Consult with the school if they have any concerns about their child's use of technology
- Support the school's approach to e-safety by not uploading or posting to the internet any pictures, video or text that could upset, offend or threaten the safety of any member of the school community or bring the school into disrepute

9. Responding and reporting to incidents of misuse

The guidance below shows the procedure to follow when responding and reporting an e-safety incident.

The incident should be recorded on CPOMS (*if the member of staff recording the incident has difficulties using the online platform they should seek help from the e-safety coordinator or the safeguarding lead on the same day they witness the incident*).

Whilst resolving an incident those students involved may have their computer accounts suspended and/or parents contacted.



10. Procedure for dealing with recorded incidents

All members of the Fir Vale Academy Trust (FVS) community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.
In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have a dedicated username and password and appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection). USE Smoothwall filtering to monitor access.
- Record the URL (smoothwall) of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screen-shots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Fir Vale Academy Trust Actions & Sanctions
It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt

with as soon as possible in a proportionate manner, and that members of the academy community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

APPENDIX 1

Legal issues relevant to the use of ICT and communications equipment

- Computer Misuse Act 1990 [Ref 1]

This was introduced as a means of prosecuting individuals who commit some form of computer crime. Hacking, eavesdropping, deliberate virus attacks are covered. Unauthorised access to a computer is the most likely offence within the Council. Only use machines/systems, which you are authorised to use.

- Data Protection Act 1998 [Ref 2]

Individuals have rights about personal data recorded on computer and in manual files. Don't put personal data in the subject line of emails; be careful about including it in the body of the text. An individual can request access to his personal data and this includes email. There are regulations about direct marketing via email.

- Copyright, Design & Patents Act 1988 [Ref 3]

It is an offence to copy software without the author's permission. Downloading application software without permission or forwarding programs in attachments may put you in breach of this act. Some Internet sites will not let you copy material you find there Take care.

- The Defamation Act 1996 [Ref 4]

Facts concerning individuals or organisations must be accurate and verifiable views or opinions must not portray their subjects in a way that could damage their reputation. This applies to internal as well as external email. Organisations in the UK have lost court cases where internal email systems were used to defame other organisations and heavy fines were imposed.

- Sex Discrimination Act 1975 [Ref 5]
- Race Relations Act 1976 [Ref 6]
- Disability Discrimination Act 1995 [Ref 7]
- Protection from Harassment Act 1997 [Ref 8]

Accessing or distributing material which may cause offence to individuals or damage the Council's reputation may lead to a prosecution under these Acts. The fact that it is electronic does not prevent action.

- Human Rights Act 1998 [Ref 9]

The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. Under this Act a UK citizen can assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

- Obscene Publications Act 1959 [Ref 10]

All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.
'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending and offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls

within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item. The Council is the originator of the Bradford Internet & Intranet sites, or the Governing Body in the case of Voluntary Aided and Foundation schools.

- Telecommunications Act 1984 [Ref 11]

The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under section 43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

- Protection of Children Act 1978; [Ref 12]
- Criminal Justice Act 1988 [Ref 13]

These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Reference:

[Ref 1]: https://www.legislation.gov.uk/ukpga/1990/18
[Ref 2]: https://www.gov.uk/data-protection
[Ref 3]: https://www.legislation.gov.uk/ukpga/1988/48/contents
[Ref 4]: https://www.legislation.gov.uk/ukpga/1996/31/contents
[Ref 5]: https://www.legislation.gov.uk/ukpga/1975/65
[Ref 6]: http://www.legislation.gov.uk/ukpga/1976/74/pdfs/ukpga_19760074_en.pdf
[Ref 7]: http://www.legislation.gov.uk/ukpga/1995/50/contents
[Ref 8]: https://www.legislation.gov.uk/ukpga/1997/40/contents
[Ref 9]: https://www.legislation.gov.uk/ukpga/1998/42/contents
[Ref 10]: https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66/contents
[Ref 11]: https://www.legislation.gov.uk/ukpga/1984/12/contents
[Ref 12]: https://www.legislation.gov.uk/ukpga/1978/37
[Ref 13]: https://www.legislation.gov.uk/ukpga/1988/33/contents

DECLARATION:

PART 1: to be retained by staff member

This declaration refers to Fir Vale Academy Trust e-safety policy and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Anyone that use School WiFi with their own device will need to log in using their school username and password.

Declaration
You should sign two copies of this document; this copy to be retained by you. The second copy (below) is to be detached and placed in your personal file.

I confirm that I have been provided with a copy of the school's e-safety policy.
I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Name:.....

Signed:.….....

Date:. ……..

DECLARATION:

PART 2: to be detached and placed on the employee's file

This declaration refers to Fir Vale Academy Trust e-safety policy and confirms that you have been provided with a copy and that you have agreed to follow it.

All employees, supply agency staff, consultants and contractors are required to familiarise themselves with the contents of the policy on the use of ICT systems and sign the following declaration.

Anyone that use School WiFi with their own device will need to log in using their school username and password.

Declaration
You should sign two copies of this document; this copy is to be retained on your personal file.

I confirm that I have been provided with a copy of the school's e-safety policy.

I confirm that I am aware that all my electronic communications including emails and website searches may be monitored by the school and that this applies even if I am working from home on school equipment or networks.

Name: .....

Signed: .....

Date:……