FOWLER ACADEMY
EST 2015

RAINHILL
HIGH SCHOOL

RainhillSixth

# E SAFETY POLICY

FOWLER ACADEMY
EST 2015

RAINHILL
HIGH SCHOOL

RainhillSixth

# E SAFETY POLICY

| | |
|---|---|
| STATUS | NON-STATUTORY |
| RESPONSIBLE COMMITTEE | Board of Trustees |
| APPROVAL DATE | 03/07/2022 |
| RENEWAL DATE | 03/07/2025 |

SCHOOLS IN PARTNERSHIP
STEPHENSON
MULTI ACADEMY TRUST

# CONTENTS

## 1. Rationale

The use of 'Information and Communication Technologies (ICT)' has great benefits for the development of students' learning and the administration and governance of a school. With these advantages, however, come insignificant risks, including:

1.1 sexual exploitation

1.2 identity theft

1.3 spam

1.4 'cyber' bullying

1.5 Viruses

It is the aim of this policy to minimise these risks for

1.6 students

1.7 staff, Governors, Trustees and others involved with the daily activities of the school

This policy, supported by the school's acceptable use agreements for staff, governors, visitors and students (Appendix 1), is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE.

## 2. What is 'Unsafe' Use of ICT

This policy is concerned with significantly unsafe use of ICT, not minor infringements. Just as safe use of ICT is commonly known as e-safety, unsafe use of ICT is an e-safety incident. E-safety incident:

2.1 uses some form of technology

2.2 causes or could have caused significant offence, harm or distress

2.3 may or may not be deliberate

2.4 may not have occurred within school or on school equipment.

Examples of e-safety incidents (not exclusive) include:

2.5 a student or member of staff viewing pornography on a school computer

2.6 a student bullying someone from another school with text messages

2.7 a student bullying a fellow student using instant messaging services such as MSN from home

2.8 a student placing distressing posts about a member of the school community on social networking sites like Facebook

2.9 a student publishing their own address details on the internet

2.10 a student publishing revealing images of her or himself on a social networking site

2.11 a student sharing a phone video of a member of staff in a lesson with other students

2.12 a member of staff suspecting a student of being groomed by a paedophile through their use of internet chat services

2.13 a student modifying a photo of a member of staff and distributing it leading to offence

## 3. Staff Responsibilities

3.1 Network Services Manager

Maintain services in support of the safe use of ICT. Typically to include;

3.1(a) internet and email filtering and logging
3.1(b) classroom management tools to monitor ICT use
3.1(c) network access logging
3.1(d) appropriate level of network security against malicious use

3.2 Other staff

3.2(a) know what is safe use of ICT through available CPD
3.2(b) model safe use of ICT within the school community and beyond
3.2(c) be alert to unsafe use of ICT, by students & staff within school and beyond
3.2(d) manage & report incidents as appropriate
3.2(e) educate students where required by the curriculum

## 4. Student Responsibilities

4.1 Must adhere to the Acceptable Use Policy

4.2 Must report incidents as they occur through the most appropriate member of staff; current teacher, form tutor, YSM,YPL or KSPL

## 5. Parent Responsibilities

5.1 Understand this Policy and encourage their child to use ICT safely

5.2 Accept any sanctions that are applied when a student breaches the policy

## 6. Education in Safe Use of ICT

6.1 Staff

6.1(a) This will be incorporated with the 3 year refresher training in Child Protection/Safeguarding
6.1(b) New staff will receive information on the school's acceptable use policy as part of their induction
6.1(c) The school ICT Policy is available to view on the Policy platform

The training will raise awareness of their individual responsibilities for the safeguarding of children within the context of e-Safety and will cover what to do in the event of misuse of technology by any member of the school community.

### 6.2 Students

6.2(a) The school will provide opportunities through the main areas of ICT, PHSE, Citizenship, discrete ESafety lesson, national focus days and assemblies. ESafety will be supported in other curriculum areas as appropriate and other more informal settings e.g. Form Time

6.2(b) The ICT curriculum will include relevant legislation such as Data Protection and intellectual property laws which may limit what they want to do but also serves to protect them

6.2(c) Students will be taught about copyright and respecting other people's information, images, and related topics

6.2(d) Students will be made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying.

6.2(e) Students will be taught the dangers of releasing personal information through the use of social networking platforms and instant messaging / chat facilities. Where these technologies have good educational outcomes they will be available within our network services.

6.2(f) Students will also be made 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 or CEOP report abuse button

## 7. <u>Managing Technology</u>

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All internal use of the Rainhill High School, Rainhill 6th Form & FEFA network is logged to allow any inappropriate use to be identified and followed up.

### 7.1 Infrastucture

Rainhill High School and Rainhill 6th Form will monitor access and use of the school network including internet services, so activity is monitored and recorded. Email and internet activity can be monitored and explored further if required.

7.2 Managing the Internet

All access to the internet will be monitored.

Staff will make every effort to preview sites before recommending them to students; it is recognised that internet sites are beyond the control of Rainhill High School, Rainhill 6th Form and FEFA.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users should make all reasonable attempts to observe copyright of materials from electronic resources.

Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

Users must not reveal personal information about members of the school community (including names) acquired through school life on any social networking site or blog without seeking the subject's permission. Information published on the internet prior to the adoption of this policy may remain where not causing an issue, however staff should declare any material in the public domain (to the Network Manager) which will be inspected for suitability.

Collaborative learning or blogging activity must be carried out only on school managed service e.g. an internal server or hosted solution. Further advice is available from the Network Manager.

## 8. Communication

Students, Parents, Staff and Governors are made aware of the School's e-Safety Policy through a variety of means:

8.1 e-Safety messages will be embedded across the curriculum whenever the internet and/or related technologies are used including Assemblies and PHSE sessions

8.2 Parents will receive regular information regarding keeping their child safe (e safety information evenings, newsletters.

8.3 e-Safety updates will be displayed via the following methods;

8.4 8.4(a) school website
8.4(b) school learning platform
8.4(c) school screen savers

8.5 On entry to the school, students at Rainhill and FEFA sign a Home School Agreement.

## 9. Specific E-Safety Issues

Further advice available http://www.itgovernance.co.uk/

9.1 Digital images & video

Digital images are easy to capture, reproduce and publish and, therefore, misuse. It is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students. Staff should only take photographs or videos of students with the express permission of student and parent. This is normally obtained from parents on entry to the school and a list of the students whose parents have objected to this is kept by the Data Manager. It is preferred that school equipment is used for this, but in any case, images must be transferred within a reasonable time scale and solely to the school's network or hosted services controlled by the school and deleted from the original device.

Students must be advised when using their personal digital equipment, especially during field trips, that images and video should only be taken with the subjects' consent. Students should also be advised that complaints against this condition will be considered a serious breach of this policy and risk having the device confiscated until it can be inspected, in their presence, by the e-safety coordinator or a member of the Senior Leadership Team.

Permission to use images and video of all staff who work at the school is sought on induction and a copy is to be stored in the relevant personnel file.

9.2 Publishing Student's Images and Work

On a student's entry to the school, 6th Form or FEFA, all Parents/carers are asked to give permission to use their student's work / photos in the following ways:

9.2(a) on the school/FEFA web site
9.2(b) on the school's Learning Platform
9.2(c) in the school/FEFA prospectus and other printed publications that the school may produce for promotional purposes
9.2(d) recorded/ transmitted on a video or webcam
9.2(e) in display material that may be used in the school's/FEFA`s communal areas
9.2(f) in display material that may be used in external areas, ie exhibition promoting the school/FEFA
9.2(g) general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)
9.2 (h)on the school`s/FEFA`s social media pages.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by all interested parties in order for it to be deemed valid. Students' full names will not be published alongside their image by the school and vice versa. E-mail and postal addresses of students will not be published. Often, the press wishes to publish full names for members of teams. In these cases, the member of staff supervising will ensure that appropriate permission is sought. Before posting student work on the Internet, the member of staff responsible must check that permission has been given for work to be displayed.

9.3 Video Conferencing (includes Facetime)

9.3(a) All students are supervised by a member of staff when video conferencing.
9.3(b) Any conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences

9.3(c) No part of any video conference with end-points outside of the school is to be recorded in any medium without the written consent of those taking part Additional points to consider:

9.3(d) Participants in conferences offered by 3rd party organisations may not be DBS checked

9.3(e) Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference

For further information and guidance relating to Video Conferencing, please see http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

9.4 Personal Mobile Devices (PMDs) including iPads, phones and other PMDs provided by school

9.4(a) The school allows staff to bring in PMDs for their own use. Under no circumstances does the school allow a member of staff to use an identifiable PMD to contact a student using this method. Staff are advised not to contact a parent/carer using their PMD but there may be circumstances concerning a duty of care to students which override this.

9.4(b) Students are allowed to bring PMDs to school – use of these is covered by our mobile phone policy.

9.4(c) The school is not responsible for the loss, damage or theft of any personal PMD.

9.4(d) The sending of inappropriate (as determined by any involved party) text messages between any member of the school community is not allowed.

9.4(e) Permission must be sought before any image or sound recordings are made on these devices of any member of the school community

9.4(f) Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

9.4(g) Where the school provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, these devices must be used.

9.4(h) Where members of staff use PMDs to access school services such as email or the intranet, they should not download personal information such as lists of student names to their phone.

9. 9.4(i) We strongly advise the use of password protection for their PMD in case of theft, and any staff losing a PMD which is configured for school data services must report the loss to the school as soon as practical. School will then prevent further access by the device.

## 10. Further Guidance

Websites offering help and advice:

- http://www.anti-bullyingalliance.org.uk
- http://www.itgovernance.co.uk/
- http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml
- http://www.thinkuknow.co.ukc
- http://www.getsafeonline.org/
- http://www.parentscentre.gov.uk/flash/safety/main.swf
- http://www.kidsmart.org.uk/
- http://www.microsoft.com/athome/security/children/default.mspx
- http://www.parentscentre.gov.uk/

- http://schools.becta.org.uk/index.php?section=is
- http://publications.becta.org.uk/display.cfm?resID=32424&page=1835
- http://www.digizen.co.uk/
- http://www.portal.northerngrid.org/ngflportal/custom/resources_ftp/client_ftp/eSafety_audit_tool/e-Safety_audit_tool.html
- http://www.nextgenerationlearning.org.uk/safeguarding

11.2 Staff e-safety incidents

If a member of staff suspects another member of staff has breached this policy, they should report their concerns to a member of SLT. SLT will investigate to see if further action is needed and report to the Headteacher. Any internal disciplinary action taken will conform to the Staff Discipline policy. If a criminal offence has been committed, the details will be passed on to the appropriate authorities.