IT eSafety Policy – Secondary School

All Staff and Students

DISTRIBUTION	This is a Trust-wide policy and applies to all staff and students within the Trust.		
DOCUMENT ID	FT-IT004 IT eSafety Policy (All Staff & Students)		
AUTHOR	HRS	**VERSION**	2.1
RATIFIED BY THE DIRECTORS OF THE FALLIBROOME TRUST			
POLICY REVIEW CYCLE		3 YEARS	
POLICY REQUIREMENT		NON-STATUTORY	

The Fallibroome Trust, Priory Lane, Macclesfield, Cheshire, SK10 4AF
Telephone: +44 (0) 1625 827 898 | Email: info@fallibroometrust.org.uk | Web: www.fallibroometrust.org.uk

CONTENTS

INTRODUCTION

eSafety encompasses the use of new technologies, internet and electronic communications such as Learning Platforms, wireless and mobile devices, Video Conferencing, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their on-line experiences.

The school's eSafety policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection / GDPR and Security. In particular, staff and students are required to adhere to the school's IT Acceptable Use Policy (AUP).

The eSafety co-ordinator is an assigned role within each Trust school's senior leadership team.

PURPOSE

This policy aims to ensure:

- Responsible IT use by all staff and students; encouraged by education and made explicit through published policies
- Sound implementation of eSafety policy in both administration and curriculum, including secure school network design and use
- Safe and secure internet usage from an approved Internet Service Provider using suitable filtering products

GOVERNANCE

The Local Governing Body is a committee of the Fallibroome Trust. The Local Governing Body will adopt and comply with all policies communicated by the Directors of the Trust. The Local Governing Body is responsible for setting out the policies and practices for staff. The Local Governing Body may delegate these matters to:

- The Principal/Head teacher;
- A sub-committee of the Local Governing Body; or
- A sub-committee and the Principal/Head teacher.

Where this procedure refers to the Local Governing Body representative this can be any one of the above.

SCOPE

This procedure applies to all employees of the Fallibroome Trust. It is supported by several other Fallibroome Trust policies or guidelines, notably:

- FT-IT001 - Acceptable Use Policy - Staff, FT-IT002 - Acceptable Use Policy - Sixth Form, FT-IT003 - Acceptable Use Policy - Students
- FT-IT005 - Data Protection - Main Policy
- FT-IT007 - Data Protection - Data Encryption Policy
- FT-IT009 - Data Protection – Student Image Consent
- FT-IT014 - Email Policy - Staff
- Bullying and Child Protection Policies
- Staff Code of Conduct

TEACHING AND LEARNING

WHY INTERNET USE IS IMPORTANT

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils

INTERNET USE TO ENHANCE LEARNING

- The school Internet access is designed expressly for pupil and family use and includes filtering appropriate to the age of pupils.
- Pupils and families will be offered guidance regarding what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation

PUPILS WILL BE TAUGHT HOW TO EVALUATE INTERNET CONTENT

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

MANAGING INTERNET ACCESS

INFORMATION SYSTEM SECURITY

- School IT systems and security will be reviewed regularly
- Virus protection is installed across all school IT networks and is set to update automatically several times daily
- We have adopted a comprehensive security policy – see Fallibroome Data Security and Management Policy

EMAIL

- Pupils may only use approved e-mail accounts on the school systems
- Pupils must immediately tell a teacher if they receive offensive e-mail
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission
- Emails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper
- The forwarding of chain emails is not permitted

PUBLISHED CONTENT AND THE SCHOOL WEB SITE

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published
- The Principal will take overall editorial responsibility and ensure that content is accurate and appropriate

PUBLISHING PUPILS' IMAGES AND WORK

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified by their full name
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs
- Written permission from parents or carers will be checked / obtained before photographs of pupils are taken (see FT-IT009 – Data Protection – Student Image Consent) for use
- Pupil's work can only be published with written permission of the pupil and parents

SOCIAL NETWORKING AND PERSONAL PUBLISHING

- The school will block/filter access to social networking sites
- Newsgroups will be blocked unless a specific use is approved
- Pupils will be advised never to give out personal details of any kind that may identify them or their location.
- Staff will be instructed not to list students as contacts or access students on social networking sites
- Pupils and parents will be offered guidance on the use of social network spaces outside school

MANAGING FILTERING

- The school will work with the DfE and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved
- If staff or pupils discover an unsuitable site, it must be reported to the eSafety Coordinator who should be known to all members of the school community
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable

MANAGING VIDEOCONFERENCING

- IP videoconferencing activities require authorisation from the eSafety officer
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call
- Videoconferencing will be appropriately supervised for the pupils' age

MANAGING EMERGING TECHNOLOGIES

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed
- Mobile phones will not be used during lessons or formal school time for text or voice messages. The sending of abusive or inappropriate text messages is forbidden
- Staff will not use personal equipment or non-school personal electronic accounts when contacting students. They will be issued with a school phone where contact with pupils is required when possible

PROTECTING PERSONAL DATA

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and from May 2018 the General Data Protection Regulations

POLICY DECISIONS

AUTHORISING INTERNET ACCESS

- All staff must read and accept the 'Acceptable Use Policy – Staff' within the assigned time period to allow continued use of IT systems
- Where the school provides a Sixth Form Facility all students must sign and return the 'Acceptable Use Policy – Sixth Form Student' consent form to allow use of the school's IT systems
- All parents of Primary or Secondary school students must sign and return the 'Acceptable Use Policy – Primary and Secondary Student' consent form to allow use of the school's IT systems
- All staff and students may be granted Internet Access in either a supervised or an un-supervised manor. This may be revoked at any time at the discretion of the school

ASSESSING RISKS

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access
- The school will audit regularly IT provision to establish if the eSafety policy is adequate and that its implementation is effective

HANDLING ESAFETY COMPLAINTS

- Complaints of Internet misuse will be dealt with by a senior member of staff
- Any complaint about staff misuse must be referred to the Principal
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure

COMMUNITY USE OF THE INTERNET

- The school will liaise with local organisations to establish a common approach to eSafety

COMMUNICATIONS POLICY

INTRODUCING THE ESAFETY POLICY TO PUPILS

- eSafety rules and guidance will be available from the IT Department and discussed with the pupils at the start of each year
- Pupils will be informed that network and Internet use will be monitored

STAFF AND THE ESAFETY POLICY

- All staff will be given the School eSafety Policy and its importance explained
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential

ENLISTING PARENTS' SUPPORT

- Parents' attention will be drawn to the School eSafety Policy on the school website

GUIDANCE IN RESPONSE TO AN INCIDENT OF CONCERN

Risks to eSafety are, of course, caused by people acting inappropriately or even illegally. Any potential issue must be dealt with at a personal level. Teachers are the first line of defence; their observation of behaviour is essential in detecting danger to pupils and in developing trust so that issues are reported. Incidents will vary from the prank or unconsidered action to occasional extremely concerning incidents that may involve Child Protection Officers or the Police.

This section will help staff determine what action they can take within the school and when to hand the issue over to the school-based Child Protection Co-ordinator, the eSafety Officer or the Police Liaison Officer.

WHAT DOES ELECTRONIC COMMUNICATION INCLUDE?

- Internet collaboration tools: social networking sites and blogs
- Internet Research: web sites, search engines and Web browsers
- Personal Devices: mobile Phones and other mobile devices
- Internet communications: e-Mail and instant messaging (IM)
- Video Communications: webcams and videoconferencing

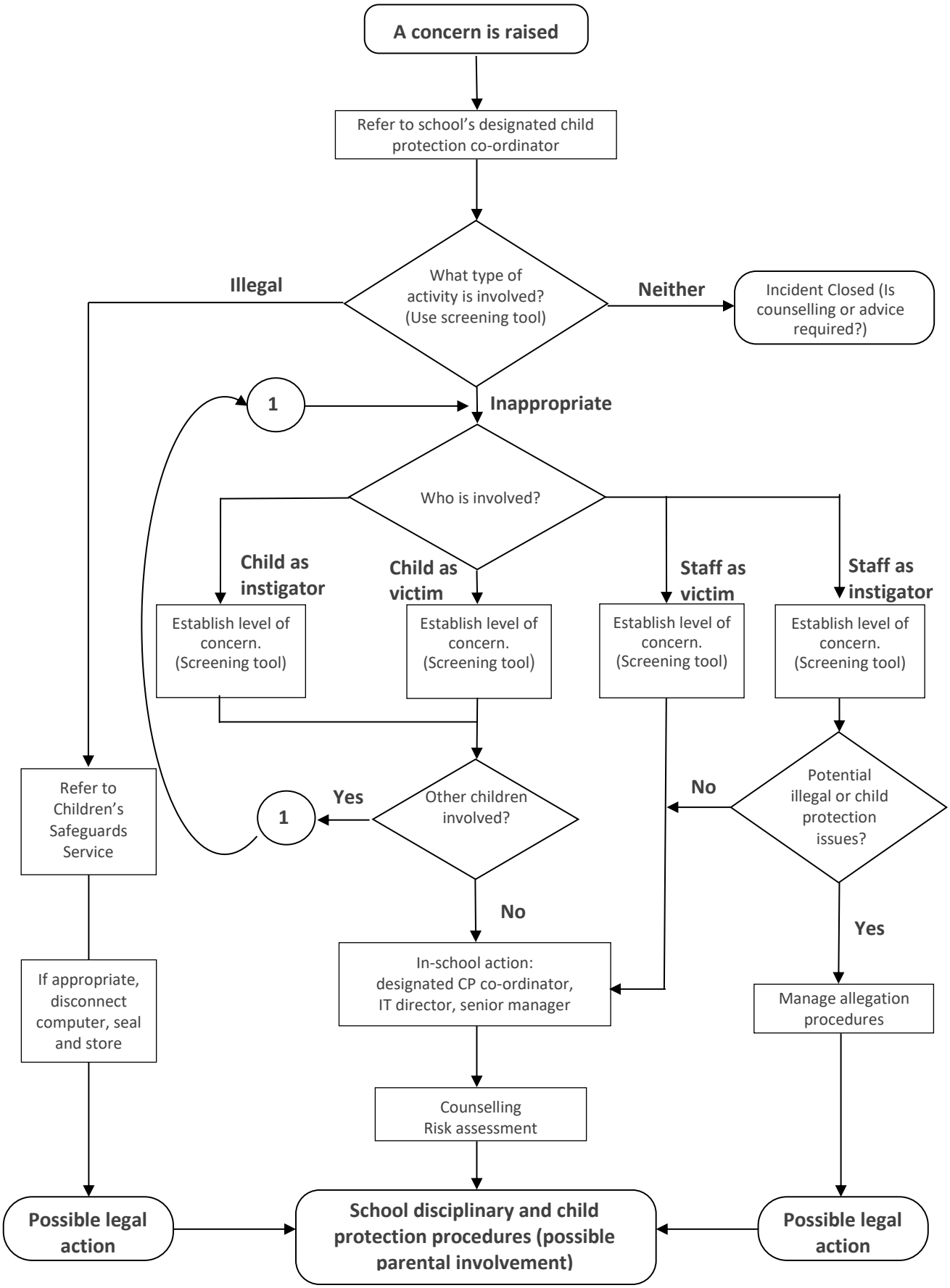
WHAT ARE THE RISKS?

- Receiving inappropriate content
- Predation and grooming
- Requests for personal information
- Viewing 'incitement' sites
- Bullying and threats
- Identity theft
- Publishing inappropriate content
- Online gambling
- Misuse of computer systems
- Publishing personal information / images
- Hacking and security breaches

HOW DO WE RESPOND?

The **Suggested Response to an Incident of Concern** flowchart on the next page illustrates the approach to investigating an incident of concern. This diagram should not be used in isolation and the Child Protection Unit and Designated staff member should be consulted.

Relevant policies (Responsible Use Policy, Behaviour Policy, Bullying Policy and Discipline Policy) are referenced and are considered when dealing with the issues identified.


A concern is raised
Refer to school's designated child protection co-ordinator
What type of activity is involved? (Use screening tool)
Illegal
Neither
Incident Closed (Is counselling or advice required?)
1
Inappropriate
Who is involved?
Child as instigator
Child as victim
Staff as victim
Staff as instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Refer to Children's Safeguards Service
1
Yes
Other children involved?
No
Potential illegal or child protection issues?
No
Yes
If appropriate, disconnect computer, seal and store
In-school action: designated CP co-ordinator, IT director, senior manager
Manage allegation procedures
Counselling
Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement)
Possible legal action

SCREENING TOOL

This screening tool can be used to assist decision making in dealing with incidents of computer or e-communications misuse. It can be used to inform initial action but is not a substitute for a thorough risk assessment / investigation.

This should be used alongside the eSafety flow chart and incidents of misuse matrix.

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit.

Type of incident

Sexual [ ]

Bullying [ ]

Violence [ ]

Incitement [ ]

Financial [ ]

Grooming [ ]

Other [ ]

How was the incident discovered?

Self-reported [ ]

Reported by 3rd party (friends or parents) [ ]

Reported by Teacher [ ]

Other (e.g. Police, Social Services, etc.) [ ]

What was their response to the incident?

Unconcerned [ ]

Curious [ ]

Distressed [ ]

Frightened [ ]

Secretive [ ]

Other [ ]

What did the incident refer to?

Answer the key questions relating to the particular incident

CHILD AS VICTIM GUIDE

Content
What was the type of content? (Sexual, violence, racial, other)
Did anyone else see it [ ]
Have they told anyone else about it? [ ]

Publishing
Is the child identifiable? [ ]
Can their location be traced/ [ ]
Is text or image potentially indecent or illegal? [ ]

Bullying
What was the type of bullying? (sexual, violent, physical, group)
Was information or images published of the child? [ ]
(If yes, refer back to publishing section for more questions to ask)

Predation / Grooming
Assess the extent of the contact
One off conversation [ ]
Regular conversation [ ]
Regular conversation using inappropriate or sexualised language or threats [ ]
Attempts to breakaway [ ]
Offline meeting arranged [ ]
Offline meeting occurred [ ]
(Consider if an offence has occurred)

Are the parents aware? [ ]
When did the incident occur?

Request for information
Did the child give out any personal information? [ ]

CHILD AS INSTIGATOR GUIDE

Content
Refer to 'Child as Victim' questions on content
Refer to the matrix to assess the child's response to the content

Incitement
Was the child secretive about the site? [ ]
Did the child access the site in an isolated place? [ ]
Did they understand the risks of accessing this site? [ ]
Was their response to the site?
Healthy (e.g. using for research) [ ]
Problematic (looking for advice or guidance) [ ]
Harmful [ ]
(Relying on site for tips, using site to communicate with likeminded individuals, the site is reinforcing /minimising potentially harmful behaviours e.g. self-harm, pro anorexia sites)

Send/Publishing
Has an offence taken place? [ ]
(Refer to glossary for information on what constitutes an offence)
Were others put at risk e.g. their image / information was sent / published [ ]
Was this an isolated incident or persistent? [ ]
Did the instigator have empathy for the victim? [ ]

Interception of communications / Hacking
Have they placed themselves or others at risk? [ ]
Has personal or financial information been stolen? [ ]
(If yes, this constitutes a criminal offence and advice should be sought from the police)
Has illegal content been accessed and sent to other's computers? [ ]

Once you have gathered the appropriate information, assess the effect of the incident on the child and identify how the child can be best supported. This may be either in school (using existing policies and resources to support children) or in certain circumstances with external help.

STAFF MISUSE GUIDE

Did the member of staff misuse the school's internal email system? [ ]

Did the member of staff communicate with a young person inappropriately [ ]
(E.g. via text message, multimedia images.)

Consider the extent of the communication@
One off conversation [ ]
Regular conversation [ ]
Regular conversation using inappropriate or sexualised language or threats [ ]
Attempts to breakaway [ ]
Offline meeting arranged [ ]
Offline meeting occurred [ ]
(Consider if an offence has occurred)

Did the member of staff access inappropriate/ illegal material within school? [ ]

Did the member of staff access inappropriate/ illegal material using [ ]
school equipment?

Did the member of staff access inappropriate/ illegal material using [ ]
their own equipment?

If you are concerned that a child may have been a victim of a criminal offence or suffered child abuse, please contact a member of the Child Protection Unit before taking any other action.

GLOSSARY

Many young people use the internet regularly without being aware that some of the activities they take part in using the internet are potentially illegal. The 2003 Sexual offences Act has introduced new offences of Grooming and raised the age for making/distributing indecent images of children to 18. Offences regarding racial hatred are covered by the Public Order Act 1986 although there is currently a new Racial and religious Hatred Bill going through parliament. Bullying etc. could be an offence under the Malicious Communications Act 1988 or Telecommunication Act 1984. Other potential offences may include Fraud (e.g. using false identities) or infringements of the Data Protection Act.

LIST OF OFFENCES:

SEXUAL OFFENCES ACT 2003

Grooming – If you are over 18 and have communicated with a child under 16 at least twice (including by phone or 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.

Making indecent images – it is an offence to take, make, distribute, show, advertise indecent images of a child under 18 (NB to view an indecent image on your computer means that you have made a digital image.)

Causing a child under 16 to watch a Sexual Act – to intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

Abuse of positions of trust. Staff need to be aware that it is 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 (Applies to teachers, social workers, health professionals, connexions Pas).

N.B. Schools should already have a copy of 'Children & Families: Safer from Sexual Crime' document as part of their child protection packs. Alternatively, information about the 2003 Sexual Offences Act can be found at www.teachernet.gov.uk

Public Order Act 1986 – offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

Telecommunications Act 1984 – Offence to send by public telecommunications network any offensive, indecent, obscene or menacing messages that cause annoyance / inconvenience / needless anxiety.

Malicious Communications Act 1988 – offence to send letter or article which includes indecent, grossly offensive, threatening or false information with the intent of causing anxiety/stress to the recipient.

Protection from Harassment Act 1997

Section 1 - 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.

Section 4 - 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.