Internet Access and Child Protection

E-Safety Policy

Fullbrook

E-Safety is part of the Fullbrook School Improvement Plan and relates to other policies including those for ICT, bullying and for Safeguarding and child protection.

Our e-Safety Policy has been written by the school, building on the Kent e-Safety Policy and government guidance. It has been agreed by senior management and approved by governors.

- ☐ The e-Safety Policy was revised by: Mrs K Moore August 2014
- ☐ It was approved by the Governors on: approval pending 8 July 2015
- ☐ The next review date is (at least annually): August 2015

Fullbrook E-Safety Co-ordinator is – Mrs K Moore
Fullbrook Designated Child Protection Officer is – Miss A Wallis
Governor with responsibility for E-Safety is Rev. M Robinson
The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)
- Internal monitoring data for network activity

Responsibilities

Role	Key Responsibilities
Principal	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security (SIRO) • To ensure the school uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident. • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

e-Safety Co-ordinator / Designated Child Protection Lead	• takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that e-safety education is embedded across the curriculum
	• liaises with school ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Governors / E-safety governor	• To ensure that the school follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the school in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)

Role	Key Responsibilities
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly
Network Manager/technician	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices • The school's policy on web filtering is applied and updated on a regular basis • That he / she keeps 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 / Officer /Headteacher for investigation / action / sanction • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures
VLE Leader	• To ensure that all data held on pupils on the VLE is adequately protected
Data Manager	• To ensure that all data held on pupils on the school office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in the curriculum and other school activities as appropriate • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws. •
All staff	• To read, understand and help promote the school's e-Safety policies and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To 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 • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.

Teaching and learning

Why the Internet and digital communications are important

The Internet, e-mail, Virtual Learning Environment and mobile computer devices are an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with high-quality Internet access, e-mail and a virtual learning environment as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.
Students use the Internet widely outside school and need to learn how to evaluate Internet information and to take care of their own safety and security.

1. Internet use will enhance and extend learning

1.1 Fullbrook Internet access is designed expressly for student use and includes filtering appropriate to the age of students at local level.

1.2 Clear boundaries will be set for the appropriate use of the Internet and digital communications and discussed with staff and students. Staff and students are made aware of these boundaries through Acceptable Use Policies which must be accepted to gain access to the internet and online services provided by Fullbrook.

1.3 Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval, evaluation and copyright, and the safe use of the Internet.

2. Students will be taught how to evaluate Internet content

2.1 Fullbrook does all it can to ensure that the use of Internet derived materials by staff and by students complies with copyright law.

2.2 Students are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy through ICT lessons at KS3.

Managing Information Systems

Although the school respects the privacy of all students and staff, Information Systems provided by the school should not be considered private. The school reserves the right to access staff or student e-mail accounts, user areas, VLE accounts or any other electronic facilities provided by the school. In circumstances where it is deemed necessary and with approval from the Principal, accounts will be accessed by the school without consent.

1. Information system security

1.1 School ICT system security will be reviewed regularly.

1.2 Virus protection is installed and updated regularly.

1.3 Security strategies will be discussed with the Local Authority as appropriate.

1.4 Students and Staff are issued with usernames and Passwords to give access to school online facilities. It is each individual's responsibility to ensure that no-one else is given access to School information systems and shall not reveal any such password to any other person.

1.5 The “master / administrator” passwords for the school ICT system, used by the Network Manager must also be available to the Principal or other nominated senior leader and kept in the school safe.

1.6 The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.

2. E-mail

2.1 Students may only use approved e-mail accounts on the school system.

2.2 Students must immediately tell a teacher if they receive offensive e-mail.

2.3 In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.

2.4 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

2.5 When using e-mail to communicate with organisations outside the school, this will be written professionally and in a business like way and, if from a student, be checked by a member of staff before sending.

2.6 The forwarding of chain letters is not permitted.

2.7 Staff will only use official school provided email accounts to communicate with students and parents/carers, as approved by the Senior Leadership Team.

2.8 Staff should not use personal email accounts during school hours or for professional purposes.

2.9 When sending e-mails to students the line manager is always to be copied in.

3. Published content and the school web site

3.1 Staff or student personal contact information will not generally be published. The contact details given online are for the school office.

3.2 The Principal or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

3.3 Fullbrook Website policy sets out procedures for information to be presented on the website.

4. Publishing students’ images and work

4.1 Photographs that include students will be selected carefully to avoid the potential for misuse of images.

4.2 Students’ full names will not be used anywhere on a school Web site in association with photographs.

4.3 Written permission from parents or carers is obtained when a students joins the school for the use of photographs of students.

5. Social networking and personal publishing

5.1 The school will control access to social networking sites in school, and consider how to educate students in their safe use.

5.2 Newsgroups and social networking sites will be blocked unless a specific use is approved.

5.3 Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

5.4 Students will be advised not to place personal photos on any social network space without considering how the photo could be used now or in the future.

5.5 Students will learn about security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.

5.6 Staff will not accept any student as a 'friend' through social media sites.

5.7 In cases where learning is taking place through the use of social media, this will be approved by the Principal and more then one member of staff will be a member of the social network learning group. Staff official blogs or wikis will be password protected and run from the school VLE with approval from the Senior Leadership Team. Members of staff are advised not to run social network spaces for student use on a personal basis.

5.8 Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and safe and professional behaviour will be outlined in the school Acceptable Use Policy for Staff.

5.9 All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.

6. Managing filtering

6.1 The school's broadband access will include filtering appropriate to the age and maturity of students.

6.2 The school will work in partnership with Surrey County Council, 4S and the Internet Service Provider to ensure that systems to protect students are reviewed and improved.

6.3 If staff or students discover an unsuitable site, it must be reported to the e-Safety Coordinator or the Network Manager.

6.4 Any material that the school believes is illegal will be reported to appropriate agencies such as Internet Watch Foundation, the Police or CEOP

7. Managing videoconferencing

Once implemented, the following will apply

7.1 IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

7.2 Students should ask permission from the supervising teacher before making or answering a videoconference call.

7.3 Videoconferencing will be appropriately supervised for the Students' age.

8. Managing emerging technologies

8.1 Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

8.2 The senior management team note that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a route to undesirable material and communications. The school policy on Personal Electronic Devices is contained in the school policy on Behaviour for Learning.

8.3 Mobile phones will not be used during lessons unless specifically directed by the teacher. The Policy regarding the use of Personal Electronic Devices in lessons is set out in detail in the School Behaviour for Learning Policy.

8.4 The sending of abusive or inappropriate text messages is forbidden.

8.5 Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in school or other officially sanctioned location.

9. Protecting personal data

9.1 Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

9.2 Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices

10. CCTV

We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without permission except where disclosed to the Police as part of a criminal investigation.
(See Fullbrook CCTV Policy)
We use specialist lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

Policy Decisions

1. Authorising Internet access

1.1 All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource and the Acceptable Use Policy for BYOD (Bring Your Own Device) before using personal devices e.g. mobile phones or tablet computers on the wireless network provided by the school.

1.2 Students are granted access to all school Information Systems and online facilities individually by agreeing to comply with the Acceptable Use Policy (AUP) statement which appears on their screens each half term when they log on.

1.3 Parents/carers should notify the school if they do not wish their son/daughter to have internet access. The school's default position is to provide all students with Internet and e-mail access to support their learning.

1.4 The school will maintain a current record of all staff and students who are NOT granted access to school ICT systems.

2. Assessing risks

1.1 The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. Neither the school nor Surrey County Council can accept liability for any material accessed, or any consequences of Internet access.

1.2 The school will audit ICT use periodically to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

3. Handling e-safety complaints

3.1 Incidents of Information Systems or Internet misuse will be dealt with by a senior member of staff, Head of Learning or Head of Faculty. The school will manage e-Safety incidents in accordance with the school's Conduct and Behaviour for Learning Policies where appropriate.

3.2 Any Incident concerning staff misuse must be referred to the Principal.

3.3 Incidents of a child protection nature must be dealt with in accordance with school safeguarding and child protection procedures.

3.4 Complaints about the school's handling of any e-Safety incidents will be handled according to the school's Complaints Procedure.

4. The community

4.1 The school will be sensitive to Internet-related issues experienced by students out of school, e.g. social networking sites, and offer appropriate advice. Note : Use of the internet outside school is not the school's responsibility.

4.2 The school will provide appropriate levels of supervision for students who use the internet and technology whilst on the school site.

4.3 The school will provide an AUP for any guest who needs to access the school computer system or internet on site.

Cyberbullying

"The rapid development of, and widespread access to, technology has provided a new medium for 'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click." DfE Preventing and Tackling Bullying. Advice for headteachers, staff and governing bodies. March 2014

1.1 Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on anti-bullying.

The Virtual Learning Environment (VLE)

1.1 SLT and staff will regularly monitor the usage of the VLE by students and staff in all areas, in particular message and communication tools and publishing facilities where these are in use.

1.2 Students/staff should apply the Acceptable use policy to their use of the VLE.

1.3 Only members of the current student, parent/carers and staff community will have access to the VLE.

1.4 All users will be mindful of copyright issues and will only upload appropriate content onto the VLE.

1.5 When staff, students etc leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment.

1.6 Any concerns about content on the VLE may be recorded and dealt with in the following ways:

a) The user will be asked to remove any material deemed to be inappropriate or offensive.
b) The material will be removed by the site administrator if the user does not comply.
c) Access to the VLE for the user may be suspended.
d) The user will need to discuss the issues with a member of SLT before reinstatement.
e) A student's parent/carer may be informed.

1.7 A visitor may be invited onto the VLE by a member of the SLT. In this instance there may be an agreed focus or a limited time slot.

1.8 Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Mobile phones and personal electronic devices

The use of mobile phones and other personal devices by students and staff in school is decided by the school and is covered in the school Behaviour for Learning Policy.
The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the school community and any breaches will be dealt with as part of the school Conduct and Behaviour for Learning Policies.

Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.

1. Students Use of Personal Devices

1.1 This is covered in detail in the School Conduct and Behaviour for Learning Policies.
1.2 Students are not allowed to bring personal devices into school under any circumstances unless the Bring Your Own Device Acceptable Use Policy has been signed and permission from the Principal sought.

2. Staff Use of Personal Devices

2.1 Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity.

2.2 Staff will be issued with a school phone where contact with students or parents/carers is required.

2.3 Mobile Phones and devices will be switched off or switched to 'silent' mode, mobile phones or devices will not be used during teaching periods unless approved for teaching and learning by the Head of Faculty.

2.4 Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.

2.5 If a member of staff breaches the school policy then disciplinary action may be taken.

Communicating e-Safety

1 Introducing the e-safety policy to students

1.1 The Acceptable Use Policy (AUP) will appear each half term when student's log on, or if there are changes to the AUP. Students are required to agree to the AUP before access is granted.

1.2 Students will be informed that network and Internet use will be monitored via the IT Code via student record books

1.3 A programme of training in e-Safety is taught thorough ICT, based on the National curriculum for Computing 2014 and for some year groups in citizenship lessons.

2 Staff and the e-Safety policy

2.1 All staff will be given the School e-Safety Policy and its importance explained. Formal e-safety training will be made available to staff as part of the planned twilight training programme for the year. All new staff will receive e-safety training as part of their induction programme during safeguarding training.

2.2 Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.

2.3 Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

2.4 Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.

3 Enlisting parents' and carers' support

3.1 Parents' and carers' attention will be drawn to the School e-Safety Policy in newsletters, the school brochure and on the school Web site.

3.2 Parents Internet Access and Child Protection Information evenings with community language support will be held annually.

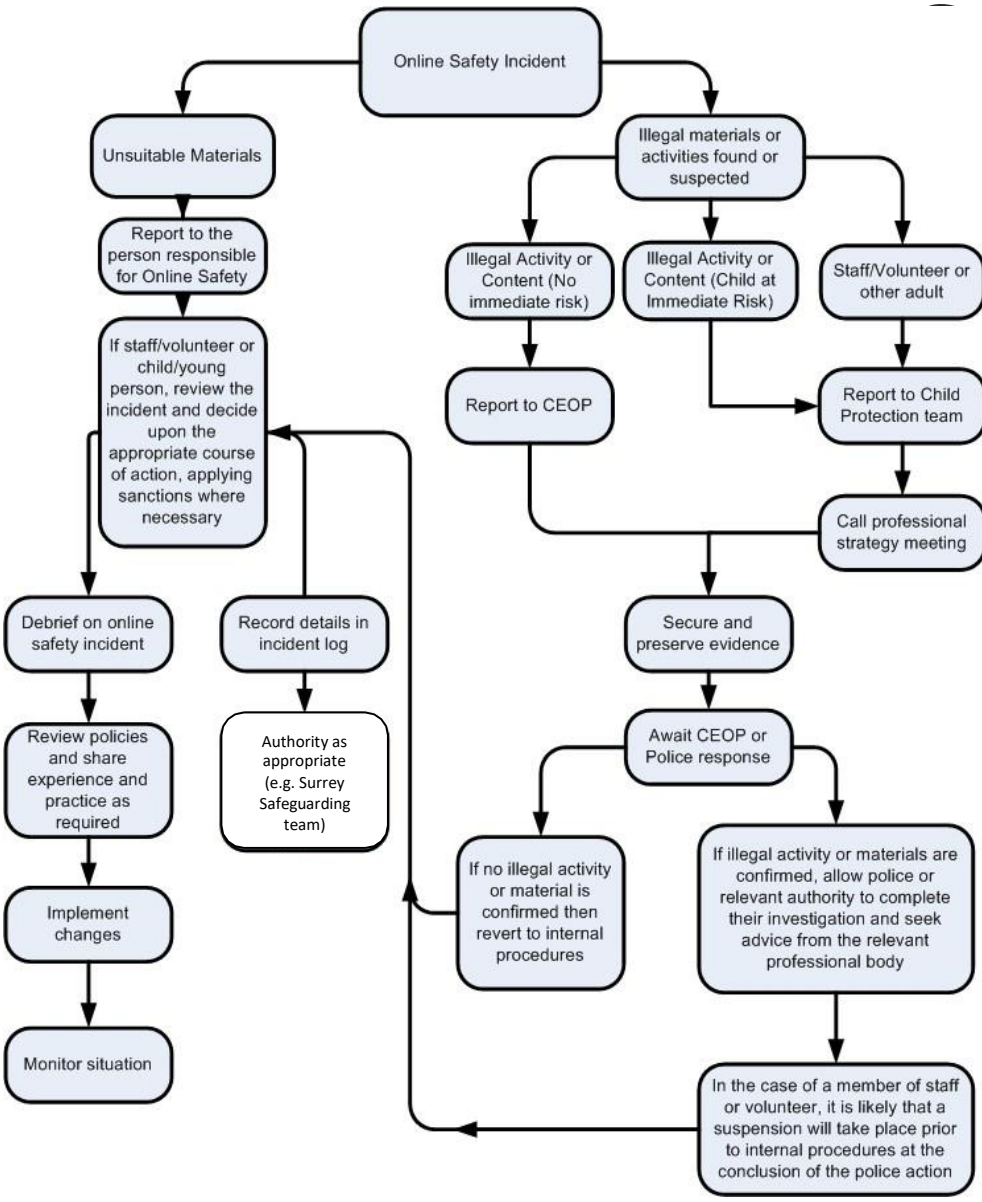
Responding to Incidents of Misuse

In cases where incidents have occurred that involve use of online services, the following processes will be followed:

1. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.

The follow chart below shows how these and other potentially illegal incidents will be handled:



2. Other Incidents

It is hoped that all members of the school 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 / network centre technician 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 appropriate Internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url (web address) 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 screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the record (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the SLT 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.

If a member of staff is found to be in breach of the e-safety policy, the disciplinary policy will be followed.

3. Incidents of misuse of IT and online services by students

Fullbrook believes it is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal conduct sanction procedures as set out in the academy conduct policy. These incidents may include the follow, though this is not an exhaustive list:

- Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities).
- Unauthorised use of non-educational sites during lessons
- Unauthorised use of mobile phone / digital camera / other mobile device
- Unauthorised use of social media / messaging apps / personal email
- Unauthorised downloading or uploading of files
- Allowing others to access academy network by sharing username and passwords
- Attempting to access or accessing the academy network, using another student's account
- Attempting to access or accessing the academy network, using the account of a member of staff
- Corrupting or destroying the data of other users
- Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature
- Continued infringements of the above, following previous warnings or sanctions
- Actions which could bring the school into disrepute or breach the integrity of the ethos of the school
- Using proxy sites or other means to subvert the academy's filtering system
- Accidentally accessing offensive or pornographic material and failing to report the incident
- Deliberately accessing or trying to access offensive or pornographic material
- Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act

e-Safety References

South West Grid for Learning E-Safety http://www.swgfl.org.uk/products-services/Online-Safety-Services/E-Safety-Resources/creating-an-esafety-policy

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Fullbrook acknowledges the use of SWGfL policy templates and e-learning materials in the development of this policy.

APPENDIX A

Network E-Safety Policy & Procedures
For Network Centre Staff

This document provides clear procedure for the handling of potentially inappropriate content on a student owned electronic device.

All E-safety incidents must be handled by a member of the Network Team in accordance with one of the three following Inappropriate Material categories:

1. **Textual materials (e.g. texts sent via BBM, Facebook messenger etc)**
   Network Action
   a) Fill in an E-Safety incident log.
   b) You may investigate on the electronic device for the inappropriate text.
   c) You may take evidence of the text via photos or screen capture software.
   d) You may re-print as required.
   e) You may store the evidence.

   Staff Action
   a) Use IRIS to appropriately report the incident.
   b) HOL will conduct further investigation as necessary and report to parents.

2. **Inappropriate images or videos that are believed to be of a person over 18**
   Network Action
   a) Fill in an E-Safety incident log.
   b) You may investigate on the electronic device.
   c) If possible ascertain who sent the image(s) or video(s) as It is a criminal offence to send or show pornography to anyone under the age of 18 (This is more directed toward Adult offenders using this to groom the student)
   d) You may take evidence of the text via photos or screen capture software.
   e) You may re-print as required.
   f) You may store the evidence in a pre-approved storage area.

   Staff Action
   a) Report this to a CP team member who will investigate further.
   b) Use IRIS to appropriately report the incident.
   c) HOL & a member of the CP team will conduct further investigation as necessary and report to parents.

   Please note: Advice from the Police recommended that a student could be a major concern if a number of images or videos are found on the electronic device and it is best to seek advice from local Police services in this case.

3. Inappropriate images or videos that are believed to be of or involving a child under the age of 18.

Initial actions

a) Confiscate the device (never allowing the device to be left unattended, unless placed in a school safe in Reception or Network)
b) Inform a CP team member immediately, they will take over the investigation.
c) DO NOT TAKE A COPY or ask network to take a copy, this is illegal.
d) According to the ACPO CPAI document section 2.5 “The ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them.”

Network Manager & relevant member of staff e.g. female photo requires a female member of staff.

a) Fill in an E-Safety incident log.
b) A review will be made on the electronic device to ascertain the severity of the content to help the CP team member.
c) The Network Manager will NOT make any copies and the police will not ask for them.
d) In the review it is important to ascertain whether the image/video was received or sent to anyone.
e) The Network Manager will only put the electronic device in the safe or give to the CP member investigating and will inform the CP member of the review.
f) Once the CP investigation is completed and it is not deemed a Police matter the Network Manager will remove the image/video from the device.
g) It is important that we record the chain of ownership for the Police. They may request this if they need to collect the device.

Incident Categorisation

This is not an exhaustive list, you should always ask advice where required.

Cyber Bullying
Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. Examples of cyberbullying include mean text messages or emails, rumour's sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Sexting
When people talk about sexting, they usually refer to sending and receiving:

- Naked pictures or 'nudes'
- 'Underwear shots'
- Sexual or 'dirty pics'
- Rude text messages or videos.

They can be sent from a friend, boyfriend, girlfriend or someone met online. They might have also sent a sexual photo, video or text to someone else.

Racism
Racism is when someone is treated differently or unfairly just because of their race or culture, people can also experience prejudice because of their religion or nationality. It is illegal to treat people differently or unfairly because of their race and nobody has the right to make you feel bad or abuse you.

Racism takes many different forms which can include:

- Written or verbal threats or insults
- Damage to property, including graffiti
- Personal attacks of any kind, including violence

Further notes:

- There is a Racial Incident Form in reception that needs to be filled in by the member of staff
- Simon Mount (PCSO) recommends looking for content that is racially aggravated to cause offence.

Sexism
Discrimination or devaluation based on a person's sex or gender

Homophobia
Homophobia is an irrational fear and hatred for homosexuality and gay and lesbian people in general.

Terrorist Material
Terrorism refers to violent acts that are intended to create fear or terror, often to achieve a religious, political, or ideological goal.

Further Note:
Simon Mount (PCSO) recommends being on the lookout for hate towards religious people or entire political parties. It is important to take into account their intention, as students may not realise what they are doing. Simon also recommends looking for racist grooming.

Electronic Grooming
Grooming is when someone builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or exploitation.
Children and young people can be groomed online or in the real world, by a stranger or by someone they know. Groomers may be male or female and they could be any age.

Many children and young people don't understand that they have been groomed, or that what has happened is abuse.

Grooming happens both online and in person. Groomers will hide their true intentions and may spend a long time gaining a child's trust. They may also try to gain the trust of the whole family so they can be alone with the child.

Groomers do this by:

- Pretending to be someone they are not, for example; saying they are the same age online
- Offering advice or understanding
- Buying gifts
- Giving the child attention
- Using their professional position or reputation
- Taking them on trips, outings or holidays.

Information Sources
This information has been taken from childline.org.uk, nspcc.org.uk, working with the Fullbrook CPLO, working with our Police Constable Support Officer, a Police Constable digital forensics expert "Simon Praine" and the ACPO CPAI lead's position on young people who post self-taken Indecent Images document (Appendix B of Fullbrook E-Safety Policy).

APPENDIX B

Association of Chief Police Officers of England, Wales and Northern Ireland

ACPO Child Protection and Abuse Investigation (CPAI) Group

ACPO CPAI Lead's Position on Young People Who Post Self-Taken Indecent Images.
1. Background.

1.1 The ACPO Lead on Child Protection and Abuse Investigation (CPAI) has released this position in response to the growing trend by young people to take and share indecent photos, not only of themselves, but also of friends and partners through SMS on mobile phones.

1.2 The taking of such photographs is often due to children and young people taking risks and pushing boundaries as they become more sexually and socially aware. With the prevalence of mobile phones with cameras and internet access and the increased use of Bluetooth technology, images can be shared easily between friends.

1.3 Sharing indecent images in this way is colloquially known by the term 'sexting' and it can have extremely damaging effects. In the US, a number of young people have committed suicide after images taken of them by previous partners were posted on social networking sites.

1.4 The 2010 Strategic Overview from the Child Exploitaiton and Online Protection (CEOP) Centre also identifies a wider range of 'risk taking' behaviour by children, including making online contact with strangers. The report highlighted that it can be difficult to distinguish between self-taken indecent images resulting from grooming or facilitation by adult offenders who have a sexual interest in children, from the images that result from children and young people simply pushing boundaries and experimenting with their friends.

1.5 An image on the internet has no natural lifespan; once posted an image may be copied by many others including those who may be predatory abusers. CEOP is aware of cases where self-taken indecent images (which were not produced as a result of grooming or facilitation) have ended up on paedophile chat sites and forums.

1.6 Crimes involving child abuse images fall under Section 1 of the Protection of Children Act 1978, as amended by section 45 of the Sexual Offences Act 2003 to extend the definition of children from under 16s to under 18s. It is a crime to take, make, permit to take, distribute, show, possess, possess with intent to distribute, or to advertise indecent photographs or pseudo-photographs of any person below the age of 18.

1.7 The consequences of this are far reaching. A prosecution for any of these offences means that an offender is placed on the sex offenders register for a duration that is commensurate with the sentence they receive. Even though the times are generally reduced for those aged younger than 18, this can still mean in some cases a considerable time spent on the register.

1.8 First time offenders should not usually face prosecution for such activities, instead an investigation to ensure that the young person is not at any risk and the use of established education programmes should be utilised. CEOP accept that in some cases, e.g. persistent offenders, a more robust approach may be called for- for example the use of reprimands. It is recommended that prosecution options are avoided, in particular the use legislation that would attract sex offender registration.

1.9 CEOP has become aware that, in certain circumstances, there is a risk that police forces may focus too narrowly on the criminal justice element of self-taken indecent images rather than wider safeguarding issues.

1.10 Although there is no evidence of this occurring in significant numbers in the UK, CEOP is aware of cases in the US where teenagers have been prosecuted for sending indecent images of themselves to friends and partners. The risk is that a purely criminal justice focused approach to this problem may result in the prosecution of children in the UK.

ACPO CPAI Position: Criminalisation of children and young people uploading self-taken indecent images.

2.1 A factor that appears to drive the creation of self-taken images is children and young people's natural propensity to take risks and experiment with their developing sexuality. This is linked to, and facilitated by, the global escalation in the use of the internet, multi media devices and social networking sites. Children and young people may not realise that what they are doing is illegal or that it may be potentially harmful to them in the future.

2.2 The reasons why children and young people post sexual images of themselves will vary from child to child. A child would not usually be in possession or be distributing these images because they have an inappropriate sexual interest in children - rather in the majority of cases, it will be as a result of their normal teenage sexual development combined with risk-taking behaviour. The recommendation is that these cases should be dealt with on a case by case basis, but within a wider safeguarding framework.

2.3 Children and young people creating indecent images of themselves may be an indicator of other underlying vulnerabilities, and such children may be at risk in other ways. At the very least, children in this situation are making themselves vulnerable due to the potential future sharing of their images. As per current ACPO Investigating Child Abuse Guidance (2009), any such minor offending behaviour by children and young people should result a referral to children's social care so that any issues that are present can be dealt with at an early stage.

2.4 Clearly some self-taken indecent images will be as a result of grooming and facilitation by adult offenders. The primary purpose of police involvement in these cases should be to ensure that the potential contact with adult exploiters is properly explored. As per Department for Education guidance, the focus of investigations should not be on the behaviour of children who have been the victims of abuse or exploitation but on the adult offenders who '*coerce, exploit, and abuse children and young people'*[1].

2.5 ACPO does not support the prosecution or criminalisation of children for taking indecent images of themselves and sharing them. Being prosecuted through the criminal justice system is likely to be distressing and upsetting for children, especially if they are convicted and punished. The label of 'sex offender' that would be applied to a child or young person convicted of such offences is regrettable, unjust and clearly detrimental to their future health and wellbeing.

2.6 ACPO considers that a safeguarding approach should be at the heart of any intervention. This approach is informed by Section 1(1) of the Children Act 1989, which states that within the context of any statutory intervention the welfare of the child is paramount. This approach is reinforced by Section 11 of the Children Act 2004, which places a duty on key persons and bodies to make arrangements to safeguard and promote the welfare of children.

2.7 Should forces require any further advice on a specific case they are encouraged to contact the Child Exploitation and Online Protection (CEOP) Centre.

[1] Department for Education; *Working Together to Safeguard Children, Safeguarding Children and Young People from Sexual Exploitation*; Supplementary guidance 'Responsibility for Criminal Acts', paragraph 2.9

APPENDIX C

Fullbrook E- Safety Incident Log

Lead Staff Name			
Network Member			
Details of incident			
Time		Date	
What device is involved			
Where did the incident occur			
Who was involved in the incident			
Names of those involved			
Type of Incident	ϒ Cyber bullying or Harassment ϒ Sexting ϒ Deliberately bypassing security or access ϒ Hacking or virus propagation ϒ Racism ϒ Sexism ϒ Homophobic material ϒ Religious hate material ϒ Terrorist material ϒ Other (Please Specify _____		
Nature of incident	ϒ Deliberate ϒ Accidental		
Did the incident involve material being	ϒ Created ϒ Viewed ϒ Printed ϒ Shown to others ϒ Transmitted to others ϒ Distributed		
Could this incident be considered	ϒ Harassment ϒ Grooming ϒ Cyberbullying ϒ Sexting ϒ Breach of AUP ϒ Other (Please Specify) _____		

Detailed Description of incident	
Actions taken	

Network Signature		Print Name	
		Date	

Lead Staff Signature		Print Name	
		Date	