BIDDULPH HIGH SCHOOL

POLICY for E-SAFETY
MRS N HARTE
REVIEWED: SEPT 2023
REVIEW DATE: SEPT 2024

Potteries Educational Trust

This policy and its procedures will be reviewed every year to ensure they are up to date, reflect current best practice and are working effectively.

Any changes that are to be incorporated into instruction and training arrangements will be effectively communicated to employees and other relevant parties.

Other related policies include:

- Social Media Policy
- ICT Policy
- Anti-bullying Policy (for more information about Cyberbullying)

---

1. INTRODUCTION

1.1 Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

1.2 Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

1.3 At Biddulph High School, we understand the responsibility to educate our students on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.4 Both this policy and the Acceptable Use Agreement (for all staff, trustees, visitors and students) are inclusive of both fixed and mobile internet; technologies provided by the Academy (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.); and technologies owned by students and staff, but brought onto Academy premises (such as laptops, mobile phones, camera phones, iPads, tablets, PDAs and portable media players, etc.).

---

2. ROLES AND RESPONSIBILITIES

2.1 As e-Safety is an important aspect of strategic leadership within the Academy, the Headteacher and trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The named e-Safety co-ordinator in our Academy is Mrs C Carroll-Wright who has been designated this role as a member of the Leadership Group. All members of the Academy community have been made aware of who holds this post. It is the role of the e-Safety co-ordinator to keep abreast of current issues and guidance through organisations such as the DFE, CEOP (Child Exploitation and Online Protection) and Childnet.

2.2 The Leadership Group and Trustees are updated by the Head/e-Safety co-ordinator and all trustees have an understanding of the issues and strategies at our Academy in relation to local and national guidelines and advice.

2.3 This policy, supported by the Academy's acceptable use agreements for staff, trustees, visitors third parties and students is to protect the interests and safety of the whole school community. It is linked to the following mandatory Academy policies: Child Protection/Safeguarding Policy; Health, Safety & Welfare Policy; Home School Policy; Behaviour & Discipline Policy; Anti-Bullying Policy and PHSE lessons.

2.4 e-Safety Skills Development for Staff.

2.5 Our staff receive information and training on e-Safety issues in the form of Staff meetings, Inset/staff training, information sheets, morning briefings and email.

2.6 New staff receive information on the Academy's acceptable use policy as part of their induction.

2.7 All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the Academy community (see attached flowchart).

2.8 All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

2.9 Managing the Academy e-Safety Messages.

2.10 We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

2.11 The e-Safety policy will be introduced to the students at the start of each academic year.

2.12 e-Safety posters will be displayed.

2.13 All students receive e-Safety awareness assemblies.

---

3. E-SAFETY IN THE CURRICULUM

3.1 ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students on a regular and meaningful basis. e-Safety is embedded within our curriculum and we continually look for new opportunities to promote e- Safety.

3.2 Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

3.3 Students are made aware of the risk and dangers of contacting strangers via the internet. Through termly assemblies and their PSHE programme, advice and guidance is provided on staying safe while using the internet. Guidance and information is provided from the Child Exploitation and Online Protection Centre. Further information is available at *http://www.ceop.police.uk/*

3.4 Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.

3.5 Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also 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/ EOP report abuse button.

---

4. PASSWORD SECURITY

4.1 Password security is essential for staff, particularly as they are able to access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

4.2 All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the Academy's e-Safety Policy.

4.3 Users are provided with an individual network and email. They are also expected to use a personal password and keep it private.

4.4 Students are not allowed to deliberately access on-line materials or files on the Academy network, of their peers, teachers or others.

4.5 If you think your password may have been compromised or someone else has become aware of your password report this to Support Manager, Mr Latham.

4.6 Staff are aware of their individual responsibilities to protect the security and confidentiality of Academy networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically.

4.7 In our Academy, all ICT password policies are the responsibility of the Support Manager, Mr Latham, and all staff and students are expected to comply with the policies at all times.

---

5. DATA SECURITY

5.1 The accessing and appropriate use of Academy data is something that the Academy takes very seriously.

5.2 Staff are aware of their responsibility when accessing Academy data. Level of access is determined by the Headteacher.

5.3 Any personal student (not assessment data) data taken off the Academy premises must be encrypted or password protected.

5.4 Data can only be accessed and used on Academy computers or laptops. Staff are aware they must not use their personal devices for accessing any *Academy/ children/ student* data. Sensitive information

and files which contain personal data should always be encrypted. If sensitive information is sent to another party, the files/information should be password protected.

---

6. MANAGING THE INTERNET

6.1 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 use of the internet is monitored by Impero Software which is installed on all machines belonging to the Academy It is monitored in real time for inappropriate use and any misuse is reported to a member of Leadership Group. Students will have supervised access to Internet resources (where reasonable) through the Academy's fixed and mobile internet technology. Staff will preview any recommended sites before use. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.

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

---

7. INFRASTUCTURE

7.1 Biddulph High School Academy has a monitoring solution called Impero supplied by Future Digital where web-based activity is monitored and recorded. This also records and monitors key words which might be used in bullying or activities of a sexual nature. The information is logged and investigated by the Leadership Group and/or the Learning Managers This monitoring is also installed on staff machines owned by the Academy.

7.2 Academy internet access is controlled through the Staffordshire Local Authority's web filtering service.

7.3 Staff and students are aware that Academy based email and internet activity is monitored and explored further if required.

7.4 The Academy does not allow students access to internet logs.

7.5 The Academy uses management control tools for controlling and monitoring workstations.

7.8 If staff or students discover an unsuitable web site the incident should be reported immediately.

7.9 It is the responsibility of the Academy, by delegation to the Support Manager, to ensure that Anti-virus protection is installed and kept up-to-date on all Academy machines.

7.10 Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the responsibility of the Academy's or the network manager to install or maintain virus protection on personal systems.

---

8. MOBILE TECHNOLOGIES

8.1 Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones

are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for education benefit and the risk assessed before use in the Academy is allowed. Our Academy chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

8.2 Personal or Academy mobile devices (including phones).

8.3 The Academy allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the Academy allow a member of staff to contact a student or parent/ carer using their personal device (e.g. Blackberry, iPhone).

8.4 Students are allowed to bring personal mobile devices/phones to the Academy but must not use them within the Academy premises. The exception to this is the 6th Form Students. They are not allowed to use phones in class or public areas.

8.5 The Academy is not responsible for the loss, damage or theft of any personal mobile device.

8.6 The sending of inappropriate text messages between any member of the school community is not allowed.

8.7 It is strictly forbidden to take any image or sound recordings on these devices of any member of the Academy community.

8.8 Users bringing personal devices into the Academy must ensure there is no inappropriate or illegal content on the device.

8.9. Users with special needs may request to bring a laptop/notebook into school to use during lesson time. This is strictly by prior arrangement only and must be discussed with the eLearning Co-ordinator. There will be no access to the school network allowed on these devices,

---

9. MANAGING EMAIL

9.1 The use of email within most schools is an essential means of communication for both staff and students. In the context of the Academy, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within the Academy or international. We recognise that students need to understand how to style an email in relation to their age and good 'netiquette'. In order to achieve ICT level or above, students must have experienced sending and receiving emails.

9.2 The Academy gives all staff their own email account to use for all Academy business. This is to minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

9.3 It is the responsibility of each account holder to keep the password secure.

Under no circumstances should staff contact students, parents or conduct any Academy business using personal email addresses.

9.4 E-mails sent to external organisations should be written carefully before sending, in the same way as a letter written on Academy headed paper.

9.5 The forwarding of chain letters is not permitted in the Academy.

9.6 All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.

9.7 Students must immediately tell a teacher/ trusted adult if they receive an offensive e-mail.

9.8 Staff must inform (the e-Safety co-ordinator/Line Manager) if they receive an offensive e-mail.

9.9 Students are introduced to email as part of the ICT Scheme of Work.

---

10. SAFE USE OF IMAGES

10.1 Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that 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.

10.2 With the written consent of parents (on behalf of students) and staff, the appropriate taking of images by staff and students with Academy equipment is permitted

10.3 Staff are permitted to use personal digital equipment, such as cameras, to record images of students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the Academy's network and deleted from the staff device.

10.4 Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of the others, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken using Academy devices provided they are transferred immediately and solely to the Academy's network and deleted from the student's device.

10.5 Consent of adults who work at the Academy

Permission to use images of all staff who work at the Academy is sought on induction and a copy is located in the personnel file.

10.6 Publishing students' images and work

On a child's entry to the Academy, all parents/guardians will be asked to give permission to use their child's work/photos:

- This consent form is considered valid for the entire period that the child attends this Academy 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.
- E-mail and postal addresses of students will not be published.
- Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

10.7 Storage of Images

10.8 Images/ films of children are stored on the Academy's network. Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher.

10.9 Webcams and CCTV

10.10 The Academy uses CCTV for security and safety. The only people with access to this are:

- Support Manager – Mr P Latham
- Headteacher – Mrs E Robinson

10.11 Notification of CCTV use is displayed at the front of the Academy.

10.12 We do not use publicly accessible webcams in the Academy.

---

11. MISUSE AND INFRINGEMENTS

11.1 Complaints

Complaints relating to e-Safety should be made to the e-Safety co-ordinator or the Headteacher. Incidents should be logged and the Flowcharts for Managing an e-Safety Incident should be followed.

11.2 Inappropriate material

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety co-ordinator or member of the Academy Leadership team.

11.3 Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-Safety Co-ordinator **(Mrs E Moss**), depending on the seriousness of the offence; investigation by the Headteacher, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart).

11.4 Users are made aware of sanctions relating to the misuse or misconduct by the Academy ICT User Agreement, assemblies, Parents Evenings, ICT lessons and the PSHE programme.

---

12. SEXTING (Advice and guidance taken form the Child Exploitation Agency)

It is important to be aware that young people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (include pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- Take an indecent photograph or allow an indecent photograph to be taken;
- Make an indecent photograph (this includes downloading or opening an image that has been sent via email);
- Distribute or show such an image;
- Possess with the intention of distributing images;
- Advertise; and
- Possess such images.

Incidents of sexting will be defined by Finkelhor: Aggravated or Experimental.

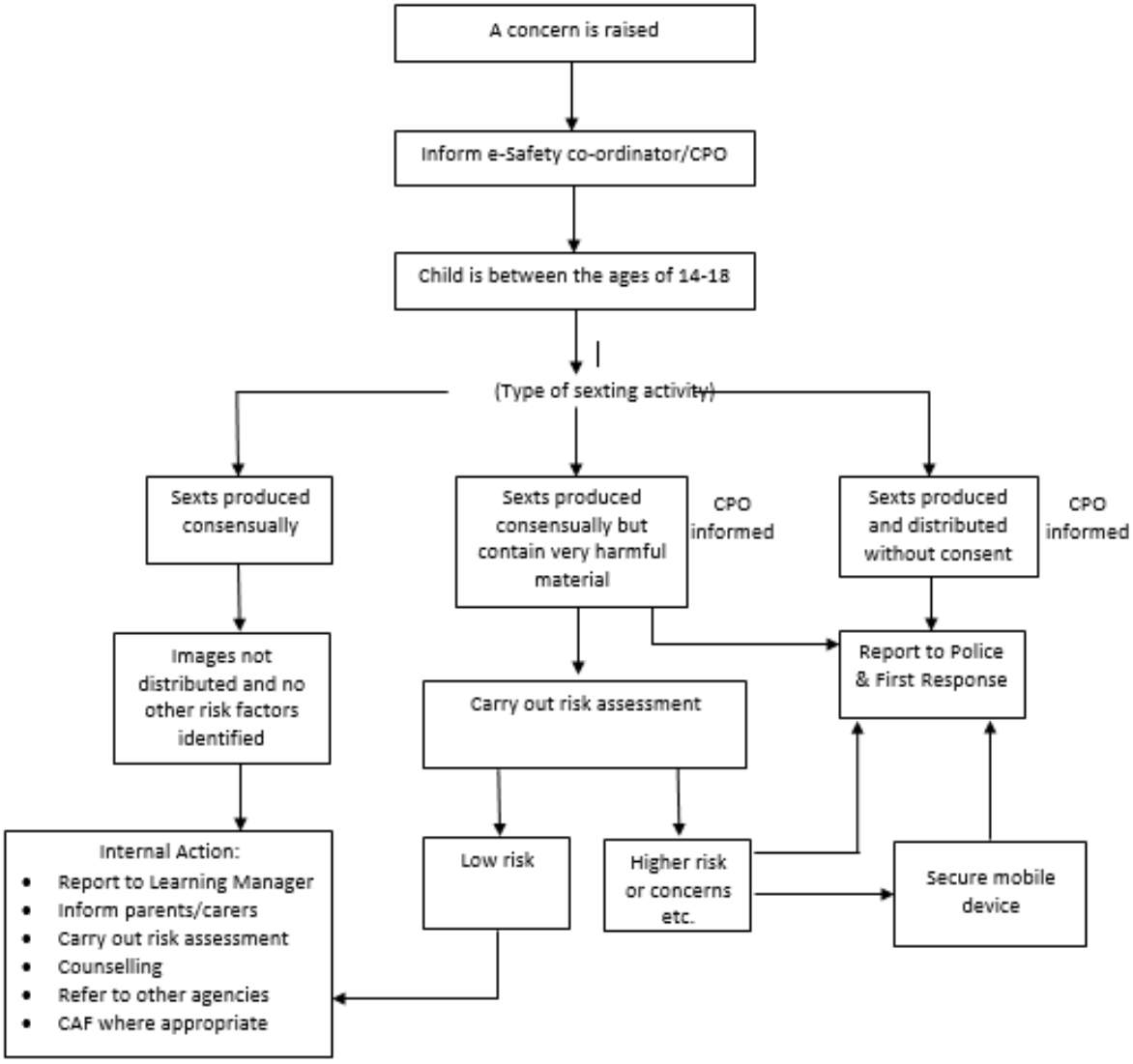
Aggravated incidents of sexting involving criminal or abusive elements beyond the creation of an image. These include further elements, adult involvement or criminal abusive behaviour by minors such as sexual abuse, extortion, threats, malicious conduct arisen from personal conflicts, or creation or sending or showing of images without the knowledge or against the will of a minor who was pictured.

Experimental incidents of sexting involved youths taking pictures of themselves to share with established boy or girlfriends, to create romantic interest in other youth, or for reasons such as attention seeking. There was no criminal element (and certainly no criminal intent) beyond the creation and sending of the images and no apparent malice or lack of willing participation.

The following sexting-response process for professionals will be used to deal with all incidents in school and the Child Protection Officer will be informed.

Appendix 1:

Sexting - Flowchart for managing a sexting incident



---

13. EQUAL OPPORTUNITIES

13.1 Students with Additional Needs

The Academy endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the Academy's e-Safety rules.

13.2 However, staff are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

13.3 Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of e-Safety. Internet activities are planned and well managed for these children and young people.

---

14. PARENTAL INVOLVEMENT

14.1 We believe that it is essential for parents/ carers to be fully involved with promoting e-Safety both in and outside of the Academy. We regularly consult and discuss e-Safety with Academy Trustees and seek to promote a wide understanding of the benefits related to ICT and associated risks.

14.2 Parents / carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the Academy.

14.3 Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g., on the Academy website).

14.4 The Academy disseminates information to parents relating to e-Safety where appropriate in the form of:

- Information and celebration evenings
- Posters
- Website
- Newsletter items

Filtering and Monitoring Standards - KCSIE

The importance of meeting the standard

Schools and colleges should provide a safe environment to learn and work, including when online. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material.

Clear roles, responsibilities and strategies are vital for delivering and maintaining effective filtering and monitoring systems. It's important that the right people are working together and using their professional expertise to make informed decisions.

How to meet the standard

Governing bodies and proprietors have overall strategic responsibility for filtering and monitoring and need assurance that the standards are being met.

To do this, the school will identify and assign:

a member of the senior leadership team and a governor, to be responsible for ensuring these standards are met

the roles and responsibilities of staff and third parties, for example, external service providers

We are aware that there may not be full-time staff for each of these roles and responsibility may lie as part of a wider role within the school, college, or trust. However, it must be clear who is responsible and it must be possible to make prompt changes to your provision.

Technical requirements to meet the standard

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

Senior leaders should work closely with governors or proprietors, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring. Your IT service provider may be a staff technician or an external service provider.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL should work closely together with IT service providers to meet the needs of your setting. You may need to ask filtering or monitoring providers for system specific training and support.

The DSL should take lead responsibility for safeguarding and online safety, which could include overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

The IT service provider should have technical responsibility for:

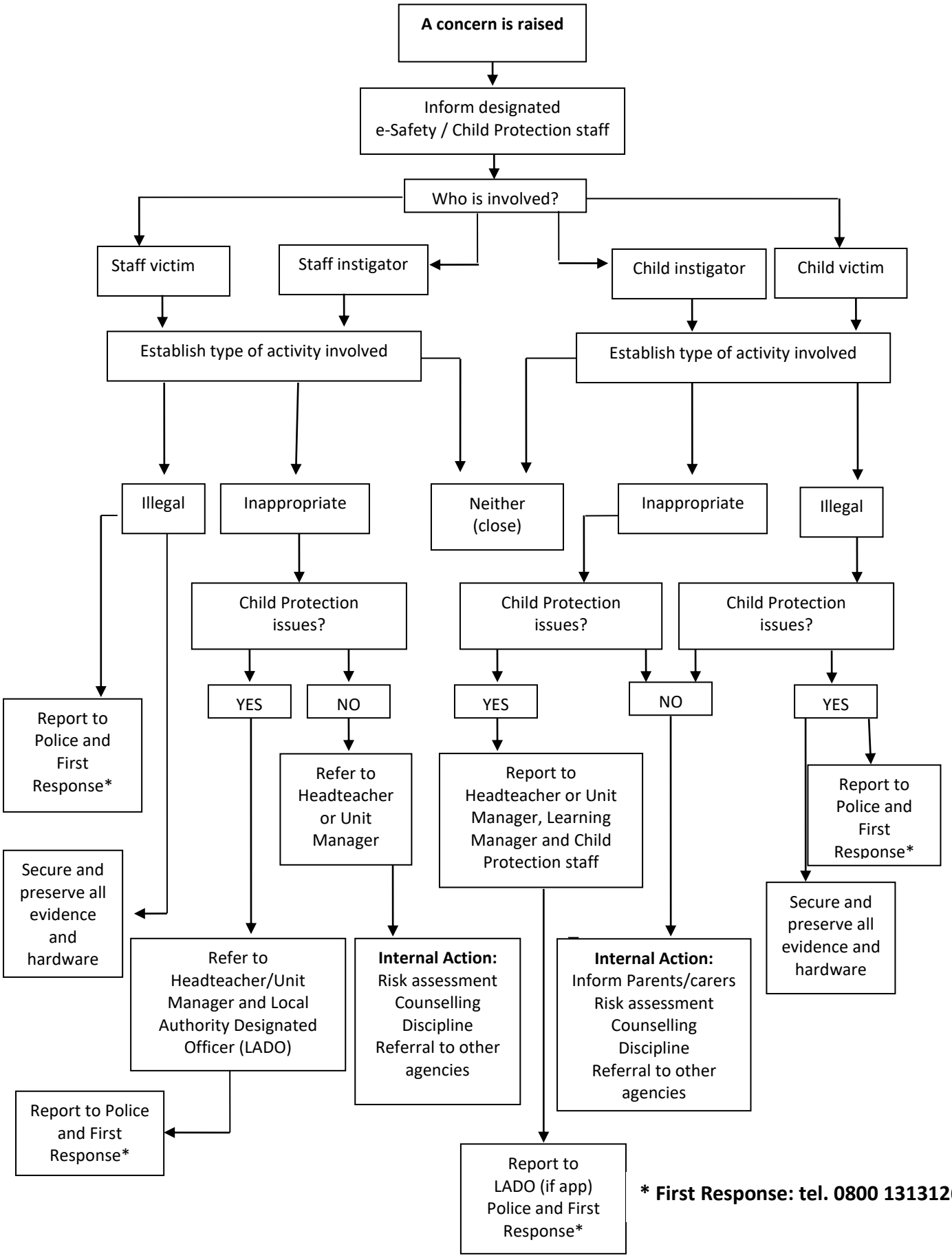
- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

Appendix 2:

Flowchart for Managing an e-Safety Incident



*** First Response: tel. 0800 1313126**

Smile and Stay Safe Poster: e-Safety Rules to be displayed next to all PCs in the Academy

and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location).

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a 'friend'.

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply.

15. CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 1998

- The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individuals' rights of access to their personal data, compensation and prevention of processing.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

- Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation. http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998 http://www.hmso.gov.uk/acts/acts1998/19980042.htm

OTHER ACTS RELATING TO E-SAFETY

Racial and Religious Hatred Act 2006

- It is a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

- The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the 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. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also 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. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

- Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

- Regardless of an individual's motivation, the Act makes it a criminal offence to gain:
  - access to computer files or software without permission (for example using another person's password to access files)
  - unauthorised access, as above, in order to commit a further criminal act (such as fraud)
  - impair the operation of a computer or program
- UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (Section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988

- Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

Public Order Act 1986 (Sections 17 – 29)

- This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

Protection of Children Act 1978 (Section 1)

- It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964

- Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997

- 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.
- 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.