LIONHEART
EDUCATIONAL
TRUST

E-SAFETY POLICY

This policy applies to all the academies in The Lionheart Educational Trust

Approved by Trust Board
January 2023 – January 2024

LHT E-Safety Policy
LHT E-Safety Co-ordinator: Victoria Foster

1. Introduction

1.1 This policy applies to all members of the Lionheart Educational Trust ("the Trust") community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the Trust ICT systems, both in and out of the Trust.

1.2 For the purposes of this policy, the term "staff" means all members of Trust staff including permanent, fixed term, and temporary staff, governors, secondees, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust in the UK or overseas. This policy also applies to all members of staff employed by any of the Trust's subsidiary companies.

1.3 The Education and Inspections Act 2006 empowers the CEO of the Trust to such extent as is reasonable, to regulate the behaviour of students when they are off the Trust site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the Trust, but are linked to membership of the Trust. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

1.4 The Trust will deal with such incidents within this policy and associated behaviour and antibullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place out of school.

2. Roles and Responsibilities

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

2.1 Trustees

The Board is responsible for the approval of the E-safety Policy and for reviewing the effectiveness of the policy. The Safeguarding Link Trustee has taken the role of e-safety Trustee. The Board will receive information about significant e-safety incidents along with monitoring reports.

2.2 Local Governing Body

The DfE guidance "Keeping Children Safe in Education" states:

"Governing bodies and proprietors should ensure there are appropriate policies and procedures in place in order for appropriate action to be taken in a timely manner to safeguard and promote children's welfare …. this includes … online safety".

Governors are responsible for the for the approval of the effectiveness of the policy e.g. by asking the questions posed in the UKCIS document "Online Safety in Schools and Colleges – questions from the Governing Body".

This review will be carried out by the safeguarding link governor who will receive regular information about online safety incidents and monitoring reports.

This will include:

i. Not limited to twice-yearly meetings with the LHT E-safety Co-Ordinator
ii. monitoring of e-safety incidents
iii. Checking that provision outlined in the Online Safety Policy (e.g. Online safety education provision and staff training is taking place as intended).
iv. reporting to relevant meeting

2.3 The Principal/Associate Principal

The Principal/Associate Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the school's E-Safety Co-ordinator.

The Principal/Associate Principal and another member of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

The Principal/Associate Principal/Senior Leaders are responsible for ensuring that the E-Safety Co-ordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.

2.4 School E-Safety Co-ordinator

The School E-Safety Coordinator:

i. takes responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
ii. ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
iii. provides training and advice for staff
iv. ensures that staff and pupils are made aware that the use of computer systems without permission or for inappropriate purpose is a criminal offence (Computer Misuse Act 1990).
v. liaises with school technical staff

2.5 Director of IT/Technical staff

The Director of IT is responsible for ensuring:

i. that the school's technical infrastructure is secure and is not open to misuse or malicious attack
ii. that the school meets required e-safety technical requirements
iii. that users may only access the networks and devices through a properly enforced password protection policy

iv. that a content filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
v. that the IT Team is up-to-date with e-safety technical information in order to effectively carry out the schools e-safety responsibilities
vi. that the use of the network/internet/Virtual Learning Environment/remote access/email is regularly monitored in order that any misuse or attempted misuse can be reported to the designated e-safety co-ordinator
vii. that monitoring systems are implemented and updated as agreed in the school policies

2.5 Teaching and Support Staff

Teaching and Support Staff are responsible for ensuring that:

i. they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
ii. they have read, understood and signed the Staff Acceptable Use Policy
iii. they report any suspected misuse or problem in accordance with all relevant policies
iv. students are aware that 'Hacking' is illegal under the Computer Misuse Act 1990. Regulations regarding unauthorised access or misuse of computing facilities are enforceable under the law, any person found attempting to or hacking the school network will be prosecuted
v. all digital communications with students/parents/carers should be on a professional level and only carried out using official school systems
vi. e-safety issues are embedded in all aspects of the curriculum and other activities
vii. students understand and follow the e-safety and acceptable use policies
viii. students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
ix. students are aware that the transmission, storage, promotion or display of offensive, defamatory or harassing material is strictly forbidden as they breach the laws of the UK under the Computer Misuse Act. Possession of certain types of unsuitable material can lead to prosecution by the police they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices
x. in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
xi. students are aware that regulations regarding the transmission, storage or display or obscene material are enforceable by law under the Criminal Justice and Public Order Act 1984 which amends the Obscene Publications Act 1956, the Protection of Children Act 1978 and the Telecommunications Act 1984 to extend their provisions to transmission over a data communications network

2.6 The Designated Safeguarding Lead (Child Protection)

The DfE Guidance "Keeping Children Safe in Education" states:

"The designated safeguarding lead should take lead responsibility for safeguarding and child protection (including online safety). This should be explicit in the role holder's job description." … Training should provide designated safeguarding leads with a good understanding of their own role, … so they … are able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and

up to date capability required to keep children safe whilst they are online at school or college."

The Designated Safeguarding Lead should be trained in e-safety issues and be aware of the potential for serious child protection/safeguarding 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

2.7 Students

Students:

i. are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy
ii. have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
iii. need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
iv. will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking/use of images and on cyber-bullying.
v. should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school

2.8 Parents/Carers

Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through Parent Teacher Day, letters, e-mail and school website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to parents' sections of the website and on-line student records
- their children's personal devices in the school

2.9 Community Users

Community Users who access school systems/website/VLE as part of the wider school provision will be expected to sign a User Contract before being provided with access to school systems.

3. Policy Statements

3.1 Education – students

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

i. A planned e-safety curriculum will be provided as part of the Digital Literacy course
ii. Key e-safety messages will be reinforced as part of a planned programme of assemblies
iii. Students will be taught in lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information
iv. Students will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
v. Students will be helped to understand the need for the Student User Contract and encouraged to adopt safe and responsible use both within and outside school
vi. Staff will act as good role models in their use of digital technologies, the internet and mobile devices
vii. In lessons where internet use is pre-planned, it is best practice that students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
viii. Where students are allowed to freely search the internet, staff should be vigilant in monitoring the content of the website's students visit
ix. It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT support team can temporarily remove those sites from the filtered list for the period of study. Any request to do so, will be auditable, with clear reasons for the need

3.2 Education – parents/carers

The school will seek to provide information and awareness to parents and carers through:

- Letters, e-mails and web site
- Parent Teacher Days
- Reference to relevant web sites and publications

3.3 Education & Training – Staff/Volunteers

The DfE guidance "Keeping Children Safe in Education" states:

"All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively."

"Governing bodies and proprietors should ensure... that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school or college safeguarding approach and wider staff training and curriculum planning."

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

i. All new staff will receive guidance on e-safety as part of their induction programme, ensuring that they fully understand this policy and the Staff Acceptable Use Policy
ii. The E-safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
iii. This E-safety policy and its updates will be presented to and discussed by staff in staff meetings/INSET days
iv. The E-safety Coordinator will provide guidance and training to individuals as required

3.4 Training – Trustees

Trustees as appropriate should take part in e-safety training/awareness sessions. Responsibility for e-safety monitoring at school level lies with the safeguarding officer for the school. The safeguarding linked Trustee is responsible for e-safety monitoring at Trust level. The senior Trust leader with responsibility for safeguarding has overall responsibility for e-safety.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority/National Governors
- Association/or other relevant organisation.
- Participation in school training sessions for staff
- Participation in online training for staff

4. Technical – infrastructure/equipment, filtering and monitoring

4.1 The DfE guidance "Keeping Children Safe in Education" states:

"It is essential that governing bodies and proprietors ensure that appropriate filters and monitoring systems are in place ...governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the … risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. "

4.2 The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy is implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities

i. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements

ii. There will be regular reviews and audits of the safety and security of the school technical systems
iii. Servers, wireless systems and cabling must be securely located and physical access restricted
iv. All users will have clearly defined access rights to school technical systems and devices.
v. All users will be provided with a username and secure password by the IT Team who will keep a record of users and their usernames. Users are responsible for the security of their username and password and are encouraged to set a secure password using the Trust recommended method of a series of unconnected words and numbers.
vi. The Director of IT is responsible for ensuring that software license logs are accurate and up to date and that regular checks are made to reconcile the number of licenses purchased against the number of software installations
vii. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered in-house using industry standard filtering equipment. Content lists are updated hourly and internet use is logged and breaches are flagged to the IT support team. Staff can raise issues with the IT support staff who can then block/unblock sites accordingly
viii. The school has multiple filtering levels. Content is appropriate for the age of each user
ix. The IT support team regularly monitor and record the activity of students on the school technical systems as explained to student in the Student Acceptable Use Policy
x. Staff are monitored in the same way as students as explained in the Staff Acceptable Use Policy
xi. An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
xii. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date anti-virus software
xiii. An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the school systems
xiv. The Staff Acceptable Use Policy states the extent of personal use that users (staff/students/community users) and their family members are allowed on school devices that may be used out of school
xv. A letter signed by staff on loan of school equipment states what can and cannot be downloaded onto the device in respect of executable files and installation of programs.
xvi. The school security policy mentions the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured
xvii. Any device brought into school and making use of the school Wi-Fi is understood to be at the owner’s risk but adheres to the same policies as any school device

5. Use of digital and video images

5.1 The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about

potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

i. When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
ii. At the Principal's discretion, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images
iii. Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the taking, storing, sharing, distribution and publication of those images
iv. Care should be taken when taking digital/video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
v. Students must not take, use, share, publish or distribute images of others without their permission
vi. Photographs that include students will only be published on the website, or elsewhere that have the correct parental consent. These images will be selected carefully and will comply with good practice guidance on the use of such images
vii. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
viii. Students' work can only be published with the permission of the student and parents/carers

6. Communications

6.1 The DfE guidance "Keeping Children Safe in Education" states:

"The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect this in their mobile and smart technology policy and their child protection policy.

6.2 A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

Communication Technologies	Staff and other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	X				X			
Use of mobile phones in lessons							X	
Use of mobile phones in social time	X				X			
Taking photos on mobile phones/cameras		X					X	
Use of other mobile devices e.g. tablets, gaming devices	X						X	
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails	X		X				X	
Use of messaging apps			X				X	
Use of social media								
Use of blogs		X					X	

6.3 When using communication technologies, the school considers the following as good practice:

i. The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)

ii. Students must immediately report to their tutor or Head of House/Year, and staff to the Principal/Associate Principal, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication

iii. Any digital communication between staff and students or parents/carers must be professional in tone and content. These communications may only take place on official school systems. Personal email addresses, text messaging or social media must not be used for these communications

iv. Students should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies

v. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

7. Social Media - Protecting Professional Identity

7.1 The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the school through limiting access to personal information:

i. Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues; phishing
ii. Clear reporting guidance, including responsibilities, procedures and sanctions
iii. Risk assessment, including legal risk

7.2 School staff should ensure that:

i. No reference should be made in social media to students, parents/carers or school staff
ii. They do not engage in online discussion on personal matters relating to other members of the school community
iii. Personal opinions should not be attributed to the school
iv. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

7.3 The school's use of social media for professional purposes will be checked regularly by the designated e-safety co-ordinator to ensure compliance with the Social Media and Data Protection Policies.

8.0 Unsuitable/inappropriate activities

8.1 The school believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The Trust policy restricts usage as follows:

User Actions Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relhte to:	**Acceptable**	**Acceptable at certain times**	**Acceptable for nominated users**	**Unacceptable**	**Unacceptable and illegal**
Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					X
Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X

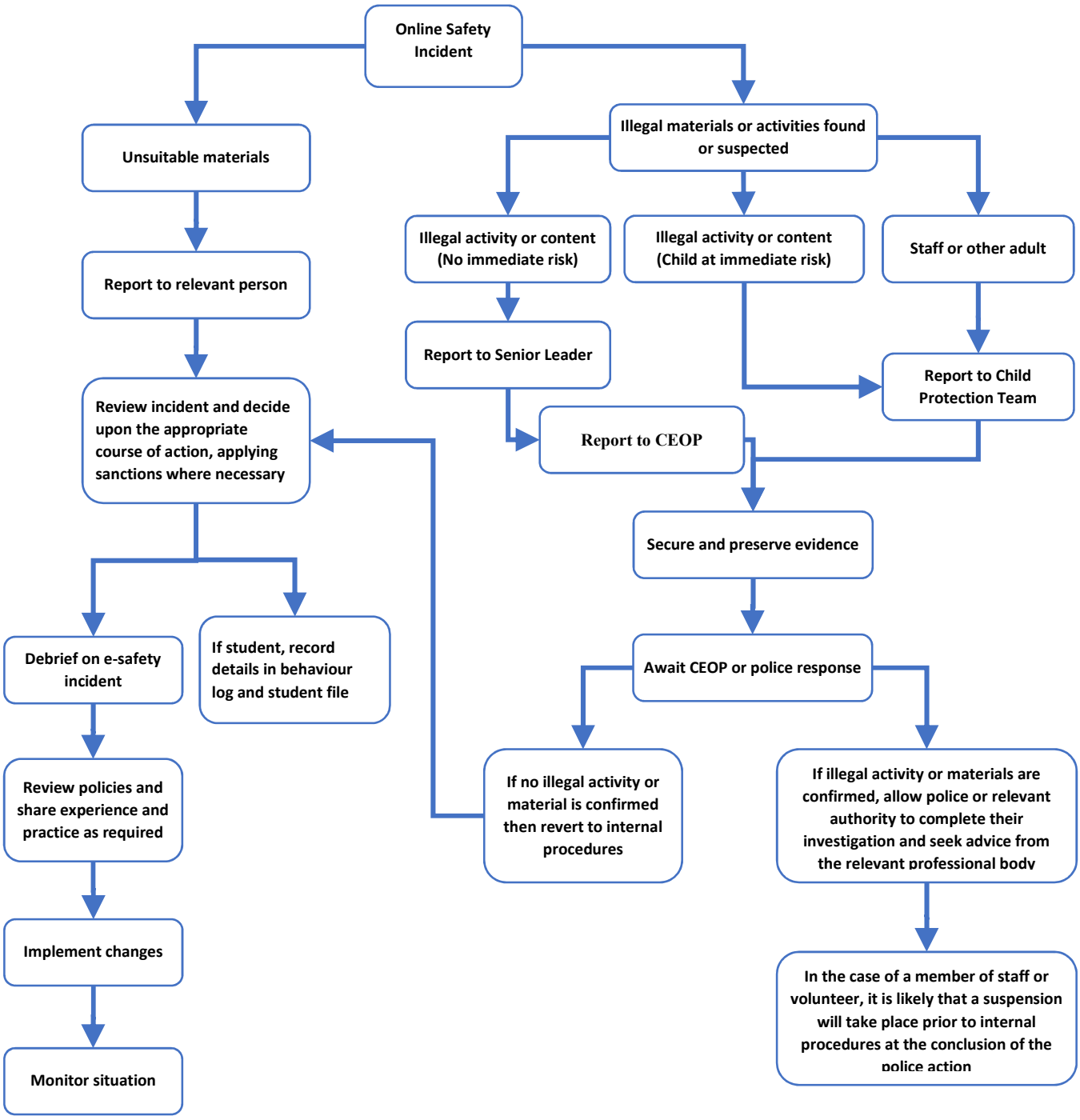
User Actions Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relhte to:	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) – contrary to the Public Order Act 1986					X
Pornography				X	
Promotion of any kind of discrimination				X	
Threatening behaviour, including promotion of physical violence or mental harm				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)			X		
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping/commerce		X			
File sharing			X		
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. Youtube		X			

9. Responding to incidents of misuse

9.1 This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities.

9.2 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 for responding to online safety incidents and report immediately to the police.



9.3 Trust Actions & Sanctions

Student Incidents:	Refer to class teacher	Refer to Safeguarding Team	Refer to Police	Refer to IT support staff for action re filtering/security etc	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. detention/exclusion
Deliberately accessing or trying to access material that could be considered illegal	X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X			X		X		
Unauthorised use of mobile phone/digital camera/other mobile device	X	X			X		X	X
Unauthorised use of social media/messaging apps/personal email	X	X		X	X	X	X	X
Unauthorised downloading or uploading of files	X			X		X		
Allowing others to access the school network by sharing username and passwords	X			X	X	X	X	
Attempting to access or accessing the school network, using another student's account	X	X		X	X	X	X	X
Attempting to access or accessing the school network, using the account of a member of staff	X	X		X	X	X	X	X
Corrupting or destroying the data of other users	X	X		X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using proxy sites or other means to subvert the school's filtering system		X		X		X	X	
Deliberately accessing or trying to access offensive or pornographic material	X	X		X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X	X	X	X	X

Staff Incidents:	Refer to line manager	Refer to Principal/Associate Principal	Refer to Human Resources	Refer to Police	Refer to IT Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal		X	X	X	X	X	X	X
Inappropriate personal use of the internet/social media/personal email	X	X				X		
Unauthorised downloading or uploading of files		X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account					X	X		
Careless use of personal data e.g. holding or transferring data in an insecure manner					X	X		
Deliberate actions to breach data protection or network security rules		X			X	X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		X	X	X	X	X	X	X
Using personal email/social networking/instant messaging/text messaging to carrying out digital communications with students	X	X						
Actions which could compromise the staff member's professional standing	X	X	X		X	X	X	X
Actions which could bring the school/academy into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X
Using proxy sites or other means to subvert the school's filtering system	X				X	X		
Accidentally accessing offensive or pornographic material and failing to report the incident	X				X			
Deliberately accessing or trying to access offensive or pornographic material	X	X	X		X	X	X	X
Breaching copyright or licensing regulhtions	X				X	X		

Repeat or serious incidents beyond the above described warnings may lead to staff disciplinary.

10. Other relevant documents

10.1 This following school guidance and policy documents are also relevant to this policy.

- Behaviour Policy
- Social Media Policy
- Data Protection Policy
- Student Acceptable Use Policy
- Staff Acceptable Use Policy