Hope Academy

A joint Catholic & Church of England Academy

Online Safety Policy

Review and approved	February 2023
Approved by	Governors
Next review due	February 2024

Contents

Statement of Intent

The Academy has provided IT facilities for teacher and student use, offering access to a vast amount of information for use in studies and offering great potential to support teaching and learning.

The IT facilities are provided and maintained for the benefit of the entire Academy community, and everyone is encouraged to use and enjoy these resources and help to ensure they remain available to all. Students are responsible for respectful behaviour with the resources and on the internet just as they are in a classroom or an Academy corridor.

Purpose

- To educate students about online safety issues and appropriate behaviours so that they remain safe and legal online.
- To help students to develop critical thinking skills to reflect and enable them to keep themselves safe.
- To keep any personal data and information secure.
- To minimise the risks of handling sensitive information.

The online safety policy links to the Academy's acceptable use policy (for students and staff), policies for child protection, anti-bullying, behaviour for learning and staff code of conduct.

Overview - Context

'All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online as well as face to face. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content'

DfE - Keeping Children Safe in Education, Sept 2022

The breadth of issues classified within online safety is considerable, but can be categorised into three areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, hate sites, violence, self-harm/suicide sites, racist or radical and extremist views;
- **Contact:** being subjected to harmful online interaction with other users (cyberbullying); for example commercial advertising as well as adults posing as children or young adults (grooming); and
- **Conduct**: personal online behaviour (digital footprint) that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images (sexting), or online bullying.
- **Commerce**: buying and selling good / services online. Risks such as online gambling, inappropriate advertising, in-app purchases, phishing and or financial scams.

The Curriculum

Online safety is delivered through the computing curriculum, enrichment opportunities (Hope Scholar Programme / iDEA Inspiring Digital Enterprise Award) and the Hope Inspire programme. Students investigate a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognise inappropriate content, contact and conduct and know how to report concerns.

Students explore the following topics: cyberbullying, digital footprint, grooming and the consequences of sexting. It is the duty of the Academy to ensure that every child in their care is safe, and the same principles should apply to the "virtual" or digital world as would be applied to the Academy's physical buildings.

This Policy document is drawn up to protect all parties – the students, the staff and the Academy and aims to provide clear advice and guidance on how to minimise risks and how to deal with any infringements.

The Technologies

ICT in the 21st Century has an all-encompassing role within the lives of children and adults. New technologies are enhancing communication and the sharing of information. Current and emerging technologies used in Hope Academy and, more importantly in many cases, used outside of the Academy by students include:

- The Internet
- e-mail
- Instant messaging (often using simple web cams)
- Blogs (an on-line interactive diary)
- Podcasting (radio / audio broadcasts downloaded to computer or MP3/4 player)
- Social networking sites
- Video broadcasting sites
- Chat Rooms
- Gaming Sites
- Music download sites
- Mobile phones with camera and video functionality
- Smart phones with e-mail, web functionality and cut down "Office" applications.
- Learning platforms / Virtual Learning Environments

Whole Academy approach to the safe use of ICT

Creating a safe ICT learning environment includes three main elements at Hope Academy:

- An effective range of technological tools;
- Policies and procedures, with clear roles and responsibilities;
- A comprehensive online safety education programme for students, staff and parents.

Roles and Responsibilities

Online safety is recognised as an essential aspect of strategic leadership in this Academy and the Principal, with the support of Governors, aims to embed safe practices into the culture of the Academy. The Principal ensures that the Policy is implemented and compliance with the Policy monitored. The responsibility for e-Safety has been designated to a member of the senior leadership team.

Our Academy **Online Safety Co-ordinators are the Senior Leadership Team, Leader of Computing and the** Designated Safeguarding Lead(s).

Our Online Safety Coordinators ensures they keep up to date with e-Safety issues and guidance through relevant organisations such as The Child Exploitation and Online Protection (CEOP). The Academy's Online Safety coordinators ensures the Principal and Governors are updated as necessary.

Governors need to have an overview understanding of Online Safety issues and strategies at this Academy. We ensure our governors are aware of our local and national guidance on e-Safety and are updated at least annually on policy developments. Staff, governors, students and parents have access to the National Online Safety resources.

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following Academy e-Safety procedures. Central to this is fostering a "No Blame" culture so students feel able to report any bullying, abuse or inappropriate materials.

Concern:	Report to:	Name:
Safeguarding	Designated Safeguarding Lead Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer Deputy Designated Safeguarding Officer	Rachel Harkness-Brennen Denise Patrick Julie Owen Marie Adams Nathan Harrison Eve Mawdsley Liam Foy Lucy Cawley
IT equipment	Network Manager	David Irving
Online Safety	Senior Leadership Team Head of Computing & Business Designated Safeguarding Lead	Marie Adams/Joe Ellis/Peter Ward Paul Bailey Rachel Harkness-Brennen

All staff should be familiar with the Academy's Policy including:

- Safe use of e-mail;
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network;
- Safe use of Academy network, equipment and data;
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras;
- Publication of student information/photographs and use of website;
- eBullying / Cyberbullying procedures;
- Their role in providing e-Safety education for students.

How will complaints regarding Online Safety be handled?

The Academy will take all reasonable precautions to ensure Online Safety. However, owing to the international scale and linked nature of internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on an Academy computer or mobile device. Neither the Academy nor the Local Authority can accept liability for material accessed, or any consequences of Internet access.

Staff and students are given information about infringements in use and possible sanctions.

Our Senior Leadership Team and Designated Safeguarding Lead acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal.

Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with Academy child protection procedures.

Managing the internet safely

Hope Academy:

- Maintains broadband connectivity through St Helens Council.
- Ensures any concerns about the system are communicated to the Academy's managed service provider (St Helens Council) so that systems remain robust and protect students;
- Ensures network health through appropriate anti-virus software etc. and network set-up so students cannot download executable files
- Ensures their network is "healthy" by having the Academy ICT technical team carry out regular audits.
- Ensures the Systems Administrator / network manager is up-to-date with services and policies;
- Ensures the Systems Administrator / network manager checks to ensure that the filtering methods are effective in practice and that they remove access to any website considered inappropriate by staff immediately;
- Never allows students access to Internet logs;
- Uses individual log-ins for students and all other users;
- Uses teacher "remote" management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Never sends personal data over the Internet unless it is encrypted or otherwise secured;
- Ensures students only publish within appropriately secure learning.

Policy procedures for teaching and learning:

Hope Academy:

- Supervises students' use at all times, as far as is reasonable, and is vigilant in learning resource areas where older students have more flexible access;
- We use an internal filtering system in conjunction with the St Helens Council filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature;
- Plans the curriculum context for Internet use to match students' ability.
- Is vigilant when conducting "raw" image search with students e.g. Google is defaulted to safe search for images.
- Informs users that Internet use is monitored;

- Informs staff and students that that they must report any failure of the filtering systems directly to the [system administrator / teacher / person responsible for URL filtering]. Our systems administrators report to LA where necessary;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform;
- Only uses approved system services for video conferencing activity;
- Only uses approved blogging or discussion sites, such as on the approved Learning Platform and blocks others.
- Only uses approved or checked webcam sites;
- Has blocked student access to music download or shopping.
- Requires students to agree to our Acceptable Use Agreement every time they log onto a computer.
- Requires all staff to agree to our Acceptable Use Agreement every time they log onto a computer.
- Makes clear all users know and understand what the „rules of appropriate use" are and what sanctions result from misuse – through staff meetings and teaching programme;
- Keeps a record of any bullying or inappropriate behaviour for as long as is reasonable in-line with the Academy behaviour management system;
- Ensures parents provide consent for students to use the Internet, as well as other ICT technologies, as part of the data collection at time of their daughter's / son's entry to the Academy;
- Makes information on reporting offensive materials, abuse / bullying etc. available for students, staff and parents when appropriate;
- Immediately refers any material we suspect is illegal to the appropriate authorities – LA / Police.

Education programme:

Hope Academy:

- Fosters a "No Blame" environment that encourages students to tell a teacher / responsible adult immediately if they encounter any material that makes them feel uncomfortable;
- Ensures students and staff know what to do if they find inappropriate web material i.e. to switch off monitor and report the URL to the teacher or IT Manager.
- Ensures students and staff know what to do if there is a cyber-bullying incident;
- Has a clear, progressive e-safety education programme throughout all Key Stages, built on LA / national guidance.

Students are taught a range of skills and behaviours appropriate to their age and experience, such as to:

- STOP and THINK before they CLICK
- THINK before they post
- expect a wider range of content, both in level and in audience, than is found in the Academy library or on TV;
- discriminate between fact, fiction and opinion;
- develop a range of strategies to validate and verify information before accepting its accuracy;
- skim and scan information;
- be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
- know search engines / websites that would to bring effective results;
- know how to narrow down or refine a search;
- [for older students] understand how search engines work;
- understand how photographs can be manipulated and how web content can attract the wrong sort of attention;

- understand "Netiquette" behaviour when using an online environment such as a "chat" / discussion forum, i.e. no bad language, propositions, or other inappropriate behaviour;
- not download any files – such as music files - without permission;
- understand why they should not post or share details of their personal lives, contact information, daily routines, photos and videos;
- have strategies for dealing with receipt of inappropriate materials.

Hope Academy:

- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must observe and respect copyright / intellectual property rights;
- Makes training on e=safety available to staff
- Runs a rolling programme of advice, guidance and training for parents
- Provides information in safety leaflets; in Academy newsletters; on the Academy web site
- Holds demonstrations, practical sessions held at the Academy - Journey of Hope - **Child Protection & Internet Safety Workshops for parents;**
- Provides suggestions for safe Internet use at home;
- Provides provision of information about national support sites for parents.

Managing e-mail safely

How will e-mail be managed?

E-mail is now an essential means of communication for staff in our schools and academies and increasingly for students and homes. Directed e-mail use in Academies can bring significant educational benefits through increased ease of communication between students and staff, or within local and international Academy projects.

However, un-regulated e-mail can provide a means of access to a student that bypasses the traditional Academy physical boundaries. The central question is the degree of responsibility for self-regulation that may be delegated to an individual. Once e-mail is available it is difficult to control its content.

Technology:

Incoming and outgoing e-mail can be restricted to approved addresses and filtered for unsuitable content and viruses. This is the first line of defence.

Where the Academy receives nuisance or bullying e-mails and the e-mail address of the sender is not obvious, it is possible to track the address using, e-mail tracking software.

Procedures:

In the Academy context, e-mail should not be considered private and the Academy reserves the right to monitor e-mail (Microsoft 365 – Outlook). There is a balance to be achieved between monitoring to maintain the safety of students and the preservation of human rights, both of which are covered by recent legislation.

The use of personal e-mail addresses, such as Hotmail / Gmail, should be avoided by all working in Academies and staff should use the Academy's systems wherever possible for professional purposes.

Education:

Students need to be made aware of the risks and issues associated with communicating through e-mail and to have strategies to deal with inappropriate e-mails. This should be part of the Academy's e-Safety and anti-bullying education programme.

Students need to understand appropriate "netiquette" style of writing, (this links to English) and appropriate e-mail behaviour appropriate to their age.

Using digitasl images and video safely

Guidelines for using digital images and video safely

Developing safe Academy websites

The Academy website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the Academy's website for information and it can be an effective way to share the Academy's good practice and promote its work. Procedures and practice need to ensure website safety.

Use of still and moving images

Most importantly, take care when using photographs or video footage of students on the Academy website. Consider using group photographs rather than photos of individual students. Do not use the first name and last name of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the Academy. An easy rule to remember is:

- **If the student is named, avoid using their photograph / video footage.**
- **If the photograph /video is used, avoid naming the student.**

If showcasing examples of students work consider using only their first names, rather than their full names.

Only use images of students in suitable dress to reduce the risk of inappropriate use.

Photographs taken for official Academy use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act 2018 / General Data Protection Regulation (GDPR). As such, students should be advised why they are being taken.

Parental permission should be obtained before publishing any photographs, video footage etc of students on the Academy website or in a DVD. This ensures that parents are aware of the way the image of their child is representing the Academy. All parents are required to complete a Parental Permission Form but this should be checked as to whether permission has been granted before images are used.

Procedures:

Use excerpts of students' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons. This allows students to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of students.

Links to any external websites should be thoroughly checked before inclusion on the Academy website to ensure that the content is appropriate both to the Academy and for the intended audience. Remember

that the content of websites can change substantially, even in a short space of time. Check all links regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by students should always be reviewed before publishing it on the Academy website. Make sure that the work doesn't include the full name of the student, or reveal other personal information, such as membership of after Academy clubs or any other details that could potentially identify them. Although it may seem obvious, check that students' work doesn't contain any statements that could be deemed defamatory.

Ensure also that the Academy is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

If the website contains any guestbook, notice board or blog, they need to be monitored to ensure they do not contain personal details of staff or students.

If showcasing Academy-made digital video work, take care to ensure that students aren't referred to by name on the video, and that students' full names aren't given in credits at the end of the film.

Technical:

Digital images / video of students need to be stored securely on the Academy network and old images deleted after a reasonable period, or when the student has left the Academy.

Hope Academy:

- The Principal takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to administration officers with the necessary administration rights as decided by the Academy's e-safety officer.
- The Academy web site complies with the Academy's guidelines for publications;
- Most material is the Academy's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the Academy address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the Academy agreement form when their daughter / son joins the Academy;
- Digital images /video of students are stored in the teachers‟ shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key Academy publication;
- We do not use students‟ names when saving images in the file names or in the <ALT> tags when publishing to the Academy website;
- We do not include the full names of students in the credits of any published Academy produced video materials / DVDs;
- Staff sign the Academy's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;

- Students are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Students are taught about how images can be abused in their eSafety education programme;

Using the academy network, equipment and data safely – General guidance

The computer system / network is owned by the Academy and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The Academy reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

To ensure the network is used safely this Academy:

- Following this, they are set-up with Internet and email access and can be given an individual network log-in username and password;
- Provides students with an individual network log-in username.
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find them;
- Makes clear that students should never be allowed to log-on or use teacher and staff logins – these have far less security restrictions and inappropriate use could damage files or the network;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and students do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music download or shopping sites – except those approved for educational purposes;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the Academy provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the Academy, is used solely to support their professional responsibilities and that they notify the Academy of any “significant personal use” as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role;
- Ensures that access to the Academy’s network resources from remote locations by staff is restricted and access is only through Academy / LA approved systems:

- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
- Provides students and staff with access to content and resources through the approved Learning Platform which staff and students access using their username and password.
- Ensures that all student level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the Academy ICT systems regularly with regard to security

Cyber-bullying policy

The Academy Anti-Bullying Policy covers cyber bullying. It makes clear that use of the web, text messages, e-mail, video or audio to bully another student or member of staff will not be tolerated.

The policy makes explicit reference to cyber bullying and includes the following guidance for staff:

"Bullying can be done verbally, in writing or images, including through communication technology (cyber bullying) e.g.: graffiti, text messaging, e-mail or postings on websites. It can be done physically, financially (including damage to property) or through social isolation. Verbal bullying is the most common form.

If a bullying incident directed at a child occurs using email or mobile phone technology either inside or outside of Academy time.

- Advise the child not to respond to the message
- Refer to relevant policies including e-safety/acceptable use, anti-bullying and PHSE and apply appropriate sanctions
- Secure and preserve any evidence
- Inform the Academy's e-safety officer

The e-safety officer may decide to:

- Inform the sender's e-mail service provider
- Notify parents of the students involved
- Consider informing the police depending on the severity or repetitious nature of offence
- Involve the safe schools officer

If malicious or threatening comments are posted on an Internet site about a student or member of staff.

The Academy's e-safety officer will be informed who will:

- Inform and request the comments be removed if the site is administered externally
- Secure and preserve any evidence
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.

Infringements and possible sanctions

How will infringements be handled?

Students

Category A infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites
- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / chatrooms, social networking sites, news groups, etc.

Possible Sanctions:

These will be applied in line with Hope Academy's Behaviour for Learning Policy (as with any other classroom misbehaviour).

Category B infringements

- Downloading copyright material.
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible Sanctions:

Removal within classroom from ICT equipment, Directorate detention, teacher / directorate contacts home, teacher to inform e-safety officer to invoke possible removal of Internet access rights for a period.

Category C infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or MSN message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material
- Any purchasing or ordering of items over the Internet
- Transmission of commercial or advertising material

Possible Sanctions:

Referral to e-safety Coordinator with possible removal of Internet and/or Learning Platform access rights for a period, e-safety officer to contact parents.

Category D infringements

- Continued sending of emails or MSN messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018 / General Data Protection Regulation (GDPR)
- Bringing the Academy name into disrepute

Possible Sanctions

Referred to e-safety officer /involvement of relevant pastoral leader/ internal seclusion / exclusion / removal of equipment / involvement of Safe Schools Police Officer.

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Misuse of first level data security, e.g. wrongful use of passwords
- Breaching copyright.

Possible Sanctions

Referred to Senior Line Manager (member of Leadership Group) /Principal. Warning given

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any Academy / Council computer hardware or software;
- Installing unlicensed software on network;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act 2018 / General Data Protection Regulation (GDPR);
- Bringing the Academy name into disrepute.

Possible Sanctions

Referred to Principal/ Governors and follow Academy disciplinary procedures; report to LA Personnel/ Human resources, report to Police

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.
- Instigate an audit of all ICT equipment by an outside agency, such as the Academy's ICT managed service providers - to ensure there is no risk of students accessing inappropriate materials in the Academy.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

How will staff and students be informed of these procedures?

- They will be fully explained and included within the Academy's e-safety / Acceptable Use Policy. All staff will be required to sign the Academy's e-safety Policy acceptance form;
- Students will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop „safe behaviours". Students will sign an age appropriate e-safety / acceptable use form;
- The Academy's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the Academy.
- Information on reporting abuse / bullying etc. will be made available by the Academy for students, staff and parents.
- Staff are issued with the "What to do if?" guide on e-safety issues.

Support and advice

Child Net – https://www.childnet.com/

Internet matters –https://www.internetmatters.org/

Keeping Children Safe in Education – DFE

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1101457/KCSIE_2022_Part_One.pdf

National Online Safety – https://nationalonlinesafety.com/

NSPCC – https://learning.nspcc.org.uk/research-resources/schools/e-safety-for-schools/

Sexting: How to respond to an incident
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/759009/Overview_of_Sexting_Guidance.pdf

Teaching Online Safety in Schools – DFE
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/811796/Teaching_online_safety_in_school.pdf

UK Safer Internet Centre- https://www.saferinternet.org.uk/

GLOSSARY:

Term	Definition
AUP	Acceptable Use Policy
CEOP	Child Exploitation and Online Protection
Different technologies	For example, websites, email, instant messaging, chat rooms, social media, mobile phones, blogs, podcasts, downloads, virtual learning platform.
Digital literacy	Digital literacy is the ability to effectively, responsibly, safely and critically navigate, evaluate and create digital artefacts using a range of digital technologies (Computing at Schools).
Encryption	Computer programme that scrambles data on devices such as laptops and memory sticks in order to make it virtually impossible to recover the original data in event of the loss of the device; schools often use this to protect personal data on portable devices.
Grooming	Online grooming is defined by the UK Home Office as: 'a course of conduct enacted by a suspected paedophile, which would give a reasonable person cause for concern that any meeting with a child arising from the conduct would be for unlawful purposes'.
ICT	Information Communication Technology
iDEA	iDEA (Inspiring Digital Enterprise Award) is an international programme that helps you develop digital, enterprise and employability skills for free. Through our series of online challenges, you can win career-enhancing badges, unlock new opportunities and, ultimately, gain industry recognised awards that help you stand out from the crowd.

national online safety	At National Online Safety, it is our mission to make the internet a safer place for children. We will achieve this through equipping school staff, parents and children with the knowledge they need to understand online dangers and how best to react should an incident arise.
Sexting	Sending and receiving of personal sexual images or conversations to another party, usually via mobile phone messaging or instant messaging.
URL	A uniform resource locator (URL) is the web address of a resource on the Internet.
AUP	Acceptable Use Policy

Monitoring and review

This policy will be reviewed by the governing board, principal, head of centre and examinations officer on an annual basis.

The scheduled review for this policy is **date**.

Appendix A

Students must click that they agree with the below Acceptable Use Agreement each time they log onto a computer.

Acceptable Use Agreement - STUDENTS

These rules will keep everyone safe and help us to be fair to others.

1. I will only use the Academy's computers for Academy work and homework, and not deliberately abuse or misuse any piece of equipment. will only delete my own files.
2. I will not look at other people's files without their permission.
3. I will keep my login and password secret.
4. I will not bring files into Academy without permission.
5. I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the Academy.
6. I will only e-mail people I know, or my teacher has approved.
7. The messages I send, or information I upload, will always be polite and sensible.
8. I will not open an attachment, or download a file, unless I have permission, or I know and trust the person who has sent it.
9. I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family, or my friends, unless my teacher has given permission.
10. I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
11. If I see anything I am unhappy with or receive a message I do not like, I will not respond to it, but I will tell a teacher / responsible adult.

By clicking OK you are agreeing to these terms and conditions.

Appendix B

Staff must click that they agree with the below Acceptable Use Agreement each time they log onto a computer.

Acceptable Use Agreement - STAFF

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

- I will only use the approved, secure email system(s) for Academy business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download any software or resources from the Internet that can compromise the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the Academy's network security and confidentiality protocols.
- I will not connect a computer or laptop to the network / Internet that does not have up-to-date version of anti-virus software.
- I will not use personal digital cameras or camera phones for transferring images of students or colleagues without permission.
- I will ensure I am aware of digital safety issues and the Academy's e-safety policy so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access Email / Internet / Intranet.
- I understand that all Internet usage will be logged and this information could be made available to my manager on request.
- I agree and accept that any computer or laptop loaned to me by the Academy, is provided solely to support my professional responsibilities and that I will notify the Academy of any "significant personal use"
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.

By clicking OK you are agreeing to these terms and conditions

Appendix C

GUIDANCE: 'WHAT DO WE DO IF?'

An inappropriate website is accessed <u>unintentionally</u> in the Academy by a child.

- Play the situation down; don't make it into a drama.
- Decide whether to report to e- safety officer and decide whether to inform parents of any students who viewed the site.
- Inform the Academy technicians and ensure the site is filtered.

An inappropriate website is accessed <u>intentionally</u> by a child.

- Refer to the acceptable use policy that was signed by the child, and apply agreed sanctions.
- Inform the Academy technicians and ensure the site is filtered if need be.

An adult uses Academy IT equipment inappropriately.

- Ensure you have a colleague with you; do not view the misuse alone.
- Report the misuse immediately to the Principal and ensure that there is no further access to the PC or laptop.
- The Academy / e-safety officer will then consider the following course of action:
- If the material is offensive but not illegal, the Academy may decide to:
    - Remove the PC to a secure place.
    - Instigate an audit of all ICT equipment by the Academy's ICT managed service providers to ensure there is no risk of students accessing inappropriate materials in the Academy.
    - Identify the precise details of the material.
    - Take appropriate disciplinary action. (contact Personnel/Human Resource
    - Inform governors of the incident.
- In an extreme case where the material is of an illegal nature:
    - Remove the PC to a secure place and document what you have done.
    - Contact the local police and follow their advice.

A bullying incident directed at a child occurs through email or mobile phone technology, either inside or outside of Academy time.

- Advise the child not to respond to the message.
- Refer to relevant policies including e-safety and anti-bullying and apply appropriate sanctions.
- Secure and preserve any evidence.

Inform the e-safety officer who will then oversee the following course of action:

- Inform the sender's e-mail service provider.
- Notify parents of the students involved.
- Inform the safe schools officer if necessary.

Malicious or threatening comments are posted on an Internet site about a student or member of staff.

- Inform and request the comments be removed if the site is administered externally.
- Secure and preserve any evidence.
- Inform e-safety officer who will:
- Send all the evidence to CEOP at ww.ceop.gov.uk/contact_us.html
- Endeavour to trace the origin and inform police as appropriate.

You are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.

- Report to and discuss with the named child protection officer in Academy **as soon as possible.**
- Advise the child on how to terminate the communication and save all evidence.

Inform the e-safety officer who will then oversee the following course of action:

- Contact CEOP http://www.ceop.gov.uk/
- Consider the involvement police and social services.

All of the above incidences must be reported immediately to the e-safety officer.

Students should be confident in a no-blame culture when it comes to reporting inappropriate incidents involving the internet or mobile technology: they must be able to do this without fear.