



Inspire Education Trust

Together we achieve, individually we grow

Online Safety Policy

Policy Date: April 2024

Review Date: April 2026

Document History

Version	Status	Date	Author	Summary Changes
V1		Oct 21	Jane Durkin	Initial draft
V2		Jan 22	Amy Husband	Page 3; Scope of Policy; para 3, line 1 addition of 'Child Protection' Page 5; under the header Child Protection, the addition of the KCSIE statement
V3		Sept 23	Rob Darling	Significant updates and links to KCSIE 2023 Links/ references to DfE Meeting Digital and Technology Standards in Schools & Colleges – 29.3.23
V4		April 2024	V Shelley	Significant updates including renaming e-safety to online safety, technical updates, exemplification of issues and links to other policies/documents and reordering of aspects
V5		Sept 2024	Rob Mushing	Further detail added on content of online safety curriculum and how links are made within the PSHE curriculum across the primary phase (pages 11 & 12)

This online policy has been developed by a working group made up of:

- Executive leadership team / senior leaders/ pastoral managers
- Online safety coordinator
- Staff – including teachers, technical staff

The school will monitor the impact of the policy using:

- Logs of reported incidents via the 'Smoothwall' internet filtering system
- Internal monitoring data for network activity
- Surveys / questionnaires of:
 - Pupils
 - Parents / carers
 - Staff

Scope of the Policy

This policy applies to all members of the academy community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of academy ICT systems, both in and outside of the academy.

This policy has been written in line with the following documentation:

- Online Safety in Schools and Colleges Questions from the Governing Board' 2022
- 'Keeping Children Safe in Education 2023',
- 'Understanding and Identifying Radicalisation Risk in your Educational Setting' 2023,
- 'Meeting Digital Standards in Schools and Colleges: Filtering and Monitoring Standards' 2023,
- 'Providing Remote Education: non-statutory guidance for schools' 2023 'Teaching Online Safety in Schools' 2019

All pupils will be taught how to keep themselves safe online through a variety of mechanisms within the structures of our academies. All staff will receive training to ensure they understand how to keep themselves and pupils safe online and this will take a variety of forms in line with published calendars across the Trust. Staff have a duty to safeguard pupils in their care both inside out outside of school. This policy should be read in conjunction with others policies as listed below:

- Safeguarding and Child Protection (staff)
- Staff Code of Conduct (staff)
- Dignity at Work Policy (staff)
- Acceptable Use of IT Policy (staff/pupils)
- PSHE Policy (pupils)
- Radicalisation/Prevent Policy (pupils)
- Behaviour Policy (pupils)
- Anti-bullying policy (pupils)
- Remote education/Online learning policy (pupils)
- Mobile phone policy (pupils)

All incidents of online safety concerns will be dealt with in line with school/trust policies to support staff and pupils to keep safe online. All schools will deploy the trustwide technical infrastructure as detailed below

Technical specifications:

Technical – infrastructure / equipment, filtering and monitoring

The trust's firewalls, have sophisticated filtering services enabled to provide content filtering services based on definitions updated in real time from the 'Global FortiGuard' database.

The system is 'Next Generation Firewall', with advanced Layer-7 filtering, 'Deep Packet Inspection', 'Application Aware Firewalling', 'Intrusion Detection and Prevention', and has been certified against the UK Safer Internet Centre criteria for content filtering in education.

The firewalls download their content filtering database in real-time from the FortiGuard Service, which includes blocking for illegal child abuse images by actively implementing the CAIC list. FortiGuard also integrates the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. In addition, FortiGuard supports content blocking by category, and as a default blocks sites and content containing discrimination, drugs/substance abuse, extremism, malware/hacking, pornography, piracy & copyrighted material, self-harm, and violence.

The trust's Digital Safeguarding monitoring service provides real-time monitoring of Windows devices within our schools for safeguarding concerns and legislative compliance.

This is achieved by the installation of the 'Smoothwall' monitoring client which examines both keyboard and desktop application for key words and phrases.

Should a word or phrase of concern be detected by the client, a screenshot is captured and sent to the DSL/DDSL/nominated person in the relevant school. Systems are then in place for addressing this through the safeguarding protocols as detailed later in this document.

The service helps to monitor, manage, and eradicate online safety issues such as:

- Cyber Bullying
- Cyber Slacking
- Abusive and threatening language used in documents, emails or chat sessions
- Racial or Sexual Harassment
- Inappropriate web site access
- Gambling, unethical or illegal practices.

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the academy:

Each academy will ensure that the relevant people named in this document below will be effective in carrying out their online safety responsibilities.

The technical team, led by the trust IT Manager will ensure the following is in place

- Academy technical systems will be managed in ways that ensure that the academy meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to academy technical systems and devices.

- All users (at KS2 and above) will be provided with a username and a secure password. Users are responsible for the security of their username and password and regular training/reminders on maintaining the integrity of this is provided for staff and students.
- The technical staff are responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- Internet access is filtered for all users.
- Academy technical staff regularly monitor and record the activity of users on the trust's technical systems and users are made aware of this in the Acceptable User Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up to date virus software.
- The provision of temporary access of "guests" (eg trainee teachers, supply teachers, visitors) onto the school systems.
- Guest access to the Wifi network is permitted with a separate secure login provided to Guests who require access to the network. The Guest network is subject to the same filters as the main network but does not have access to any of the internal network areas. The Guest login only lasts for 24 hours
- For security and accountability/licencing, staff are not permitted to use their own iTunes accounts with mobile devices. New App's must be requested and authorised before they are installed.
- Personal data unless in accordance with Data Protection Policy cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

Board of Directors/Local Governing Committee:

Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. All schools will use the trust technical infrastructure and additional internet filtering and monitoring service. Directors will receive summary information of online safety concerns provided as part of the Director Safeguarding sub-committee.

At school level, a member of the Local Governing Committee will review the processes for monitoring online safety as part of their Governor Safeguarding role. This will involve (but not be isolated to):

- meetings with the Designated Safeguarding Lead/Deputy (DSL/DDSL) which have an online safety focus
- review of key policies in place as listed above
- review of the curriculum coverage on keep themselves safe for pupils
- review of staff training
- review of reported pupil incidents and subsequent follow up
- review of reported low-level staff concerns and follow up

A record of this monitoring should be shared with the DSL/Headteacher/Director of Primary Education and made available to relevant parties via governor hub.

Headteacher and Senior Leaders:

- The Headteacher in conjunction with the DSL has a duty of care for ensuring the online safety of members of the school community; this is also a delegated responsibility to staff within the school in their day-to-day contact with pupils and one another.
- The Headteacher is aware of the procedures to be followed in the event of **both** a low-level staff concern regarding online safety **and** a serious allegation being made against a member of staff. **THIS MUST BE REPORTED TO HEAD OF PRIMARY EDUCATION / HEADTEACHER (SECONDARY)** (See E-Safety flow-chart)
- The Headteacher is responsible for ensuring that the DSL and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Executive Leadership and Senior Management Team(s) will receive regular monitoring reports from the Safeguarding teams in schools.

Our monitoring strategy should also be informed by the filtering and monitoring review. A variety of monitoring strategies may be required to minimise safeguarding risks on internet connected devices and may include:

- physically monitoring by staff watching screens of users
- live supervision by staff on a console with device management software
- network monitoring using log files of internet traffic and web access
- individual device monitoring through software or third-party services as outlined in the technical infrastructure section above.

Senior Management Team Lead and DSL:

- responsible for keeping up to date with statutory and recommended training and leads on online safety across the school
- takes day to day responsibility for online issues and has a leading role in establishing and reviewing the relevant school policies.
- ensures that all staff are aware of the procedures that need to be followed in the event of an incident taking place.
- provides training and advice for staff
- liaises with the Local Authority / relevant body
- liaises with school technical staff

- receives reports of incidents and creates a log of incidents on CPOMS to inform future developments (N.B. Headteacher to forward monitoring reports to Pastoral Lead, DSL for Governor and Director level reporting),
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs
- reports at relevant meeting of Local Governing Board
- reports regularly to Executive Leadership Team.

Technical staff:

The Technical Staff for ICT / Computing are responsible for ensuring:

- that monitoring and filtering systems are implemented and updated as agreed.
- that the use of the network, internet filtering system and email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction
- that the trust's technical infrastructure is secure and is not open to misuse or malicious attack
- that all trust schools have the appropriate filtering systems in place
- that the trust meets the required standards in line with 'Filtering and Monitoring Standards for Schools and Colleges' these can be found here:
- [Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges-filtering-and-monitoring-standards-for-schools-and-colleges)
- that users may only access the networks and devices through a properly enforced password protection policy.
- that filtering is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with technical information in order to effectively carry out their online -safety role and to inform and update others as relevant

Teaching and Support Staff:

Are responsible for ensuring that:

- they complete all training as directed by the Headteacher/DSL and read all relevant policies as directed
- they have read, understood and signed the Staff Acceptable User Policy (AUP)
- they report any suspected misuse or problem to the Headteacher/Pastoral Manager/DSL for investigation / action / sanction in line with relevant policies
- all digital communications with parents / carers should be on a professional level and only carried out using official school systems
- online safety issues are embedded in all aspects of the curriculum and other activities required to educate children and young people to build knowledge, skills and confidence with regard to online safety including learning contained within the statutory (September 2020) Relationships Education, Relationships and Sex Education (RSE) and Health Education, the Computing curriculum, Citizenship and other subjects where relevant.

- pupils understand and follow the ICT and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations at Years 5 and 6 in primary and all secondary aged pupils
- they monitor the use of digital technologies, mobile devices, cameras etc and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils 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.

Child Protection / Designated Safeguarding Lead:

Should be trained in online 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.
 - radicalisation

In line with KCSIE 2023, our online safety policy links closely with our Child Protection policy. Where any incidents regarding online safety cause serious safeguarding concern, the Designated Safeguarding Lead(s) in the academy will act in accordance with our Child Protection policy.

Online Safety Group

The Online Safety Group comprises of the DSL, ICT Subject Leader, Pastoral Lead, IT Technician and a class teacher from the alternative Key Stage to the ICT Lead and the Head of PSHE/RE. The group has responsibility for issues regarding online safety and the monitoring the Policy including the impact of initiatives. The group will also be responsible for regularly reporting to the Headteacher to enable them to report to the Local Governing Board and Directors.

Members of the group will meet with staff from other schools within the MAT and the Head of Primary Education, Head Teacher (Secondary) to support:

- the production / review / monitoring of the school Online Safety Policy / documents.
- the production / review / monitoring of the school filtering policy and requests for filtering changes
- mapping and reviewing the curricular provision – ensuring relevance, breadth and progression
- monitoring network / internet / incident logs
- consulting stakeholders – including parents / carers and the pupils about the online safety provision
- monitoring improvement actions identified through use of the 360 degree safe self review tool.

Students / pupils:

- are responsible for using the academy digital technology systems in accordance with the Pupil Acceptable Use (Secondary) and Parent/Carer Links Policy (Primary)

- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations (Year 5 and 6 primary and all secondary aged pupils)
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and have been enabled to do so through the curriculum coverage and additional opportunities such as assemblies, drop down days and parents events and communication
Will understand how they can be vulnerable online such as through grooming, sexting, phishing, scamming, radicalisation and know the strategies to address this.
- 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.
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the academy's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The academy will take every opportunity to help parents understand these issues through *parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns*. Parents and carers will be encouraged to support the academy in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- access to parents' sections of the website and on-line pupil records
- their children's personal devices in the academy (where this is allowed).

Policy Statements

Education – pupils

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's provision. Children and young people need the help and support of the school to recognise and avoid online risks and build their resilience.







Online safety should be a specific focus in the curriculum and staff should reinforce online safety messages across the curriculum being well trained to understand the range of risks/harm to which children can be potentially exposed. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:







- A planned safety online curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited

Online Safety Curriculum

Rob Mushing – MAT Primary Digital Technology Lead

- A bespoke, self-designed Online Safety curriculum is taught from Nursery to Year 6 through half termly online safety lessons.
- Six core aspects are covered across each year:

Autumn 1 	Privacy and security online	This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.
Autumn 2 	Online bullying	This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.
Spring 1 	Health, wellbeing and lifestyle	This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.
Spring 2 	Online relationships	This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.
Summer 1 	Self-image and identity online	This strand explores the differences between online and offline identity, beginning with self-awareness, shaping online identities and media influences on propagating stereotypes. It identifies effective routes for reporting and support, and explores the impact on online technologies on self-image and behaviour.
Summer 2 	Online information	This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.

	Nursery	Reception	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
AUTUMN 1 PRIVACY & SECURITY ONLINE 	What is your personal information?	Who can you share your personal information with and why?	Why are passwords important?	What makes a safe password?	What could you do when you are asked for private information?	How do companies use personal information that is stored online?	What are app permissions and why are they important?	How do you recognise whether a website or email is genuine or not?
AUTUMN 2 ONLINE BULLYING 	What can you do if someone is unkind?	What can you do if someone is unkind online?	How can you be kind online?	What is bullying? Where can online bullying take place?	How do online comments impact on people?	Why can online comments be misunderstood?	What are online comments and why can they be misunderstood?	How do you deal with online bullying and inappropriate content online?
SPRING 1 HEALTH, WELLBEING & LIFESTYLE 	What are the rules when using technology?	What are the rules when using technology?	How can we stay healthy when using technology?	What guidance is there for healthy technology use?	How can technology use be included in a healthy day?	Why are age restrictions important?	What are the pros and cons of being online?	What is persuasive design? Why is it important to take responsibility for ourselves online?
SPRING 2 ONLINE RELATIONSHIPS 	What are the ways we use to communicate with people we know?	How do we communicate with people we know using technology?	Why is it important to be considerate and kind when communicating online?	What activities need permission when using technology?	What shouldn't be shared with online friends?	What are healthy and unhealthy online behaviours?	Should we trust everyone in the online community?	What are the consequences of unhealthy behaviour online?
SUMMER 1 SELF-IMAGE & IDENTITY ONLINE 	When might you feel sad?	When might you feel sad, uncomfortable or embarrassed, offline & online?	What online situations affect our mood?	What is someone's identity?	How does information stored online show identity?	What is online reputation?	How can we create a positive digital footprint?	What stereotypes exist online?
SUMMER 2 ONLINE INFORMATION 	Where can we find out information?	How can we find out information online?	Is all online information real?	Is all online information factual?	Who does online information belong to?	Is all online information trustworthy?	Why is online information targeted?	What are the rules when copying online content?

- Half-termly lessons are supplemented by an assembly and a home learning leaflet.
- Links are made to national online safety events, including Anti-Bullying Week and Safer Internet Day.

- Planning for all aspects is informed by National Online Safety – Online Safety Lesson Plans.



Wider Curriculum

Rob Mushing – MAT Digital Technology Lead

- Within the Digital Technology Curriculum, explicit references to e-safety links are included within curriculum planners, for example permissions, safe internet use and personal data.
- Across the curriculum, learning activities involving use of online materials provide opportunities to reinforce and apply knowledge from the Online Safety Curriculum, including permissions, online information and safe internet use.

PSHE Curriculum

Donna O'Brien – MAT PSHE Lead

- Within the *Jigsaw* PSHE Curriculum, additional coverage of aspects of online safety is built into units of work within Key Stage 2:
 - Year 3-Healthy Me
 - Keeping safe and why it's important (online and off-line scenarios)
 - Year 3-Relationships
 - Keeping safe online and who to go to for help
 - Year 5-Relationships
 - Safer online communities
 - Rights and responsibilities online
 - Online gaming and gambling
 - Reducing screen time
 - Dangers of online grooming
 - SMARRT internet safety rules
 - Year 6-Relationships
 - Technology safety
 - Take responsibility with technology use
 - Year 6-Changing Me
 - Sexting



- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / PSHE/ pastoral activities/ information to parent/ carers each half term (primary) and across the year (secondary) examples below.
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.

PSHE Curriculum Map

	Autumn 1 <small>Health & wellbeing</small>	Autumn 2 <small>Living in the wider world</small>	Spring 1 <small>Relationships</small>	Spring 2 <small>Health & wellbeing</small>	Summer 1 <small>Living in the wider world</small>	Summer 1 <small>Relationships</small>
Year 7	Transition and safety Transition to secondary school Respect in School Personal safety inside and outside of school.	Developing skills and aspirations Careers Teamwork and enterprise skills Raising aspirations Goals for the future	Diversity. Peer relationships. Making and maintaining friends – Interpersonal relationships Diversity and prejudice Bullying (inc online)	Health and puberty Healthy routines – Sleep/Hygiene/Dental Puberty and emotions Periods FGM	Financial decision making Saving, borrowing, budgeting and making financial choices Ethical shopping Identifying risk	Building relationships Self-worth Romance and friendships Media influences Assertive communication
Year 8	Drugs and alcohol Alcohol and drug misuse, including types and consequences. Pressures relating to drug use	Community and careers Types of employment Employment law and discrimination Goals for my future	Discrimination. Child on Child Abuse Group Think Discrimination and HBT Racism Human Rights	Emotional wellbeing Mental health and emotional wellbeing - including body image and coping strategies Mindfulness	Digital literacy Online safety & digital literacy, media reliability Fake news Online gaming	Identity and relationships Gender identity, sexual orientation, Consent 'sexting' An introduction to contraception
Year 9	Peer influence, substance use and gangs Group think Healthy and unhealthy friendships, and gang exploitation CSE/CCE Bystander Behaviour	Setting goals Problem Solving Career options and goal setting as part of the GCSE options process	Respectful relationships Families and parenting Homelessness Conflict resolution and relationship changes	Healthy lifestyle Work/life balance Body Image. Personal safety and cancer awareness	Work experience Preparation for and evaluation of work experience Overcoming Adversity Health and Safety Online Presence	Intimate relationships/Self checks Relationships and sex education including consent, contraception, the risks of STIs, and attitudes to pornography
Year 10	Mental health Mental health and ill health Stigma, Safeguarding health, including during periods of transition or change	Financial decision making The impact of financial decisions and debt, Gambling Financial risks	Healthy relationships Consent and victim blaming Healthy relationships including LGBTQ+ relationships Online dating and Porn	Exploring influence The influence and impact of drugs, gangs, role models and the media.	Employability skills Employability skills and enterprise personality Wages Employment rights	Addressing extremism and radicalisation Communities, Belonging and challenging extremism PREVENT
Year 11	Communication in relationships Personal values, assertive communication (including in relation to contraception and sexual health), relationship challenges and abuse. Domestic abuse and coercive control.	Families Different families and parental responsibilities, pregnancy, marriage and forced marriage Adoption, Abortion, Miscarriage	NO PSHE DELIVERED DUE TO MOCK EXAMS	Next steps Revision and study skills Post 16 Employability CV writing Interview	Building for the future Stress management, including work life balance Body image Responsible health choices, and safety in independent contexts – surgery, tattoos, piercings Blood, organ, stem cell donation	YEAR 11 EXAM LEAVE

Highlighted topics are those students can be withdrawn from.

- Pupils should be helped to understand the need for the pupil Acceptable User Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use
Students are told to report any unsuitable material that is found in internet searches to their teacher who is expected to report to the DSL to ensure the site is blocked by the school. This would also be picked up through the internet filtering system and as such is unlikely to occur.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, be made well in advance, with clear reasons for the need.
- Not all sites can be removed from the filter.

Secondary IT Curriculum:

KS3 Computing

Year 7 –

Unit 1 - 01 Impact of technology – Collaborating online respectfully - respectful communication online and L6 focus 'Who are you talking to?' Who they are interacting with online? Report suspect / inappropriate behaviour

Year 8 & 9 - 05 Cybersecurity - This unit takes students on a journey of discovery about techniques used by cybercriminals to steal data, disrupt systems, and infiltrate networks. The learners will start by considering the value of their data to organisations and what they might use it for. They will then look at social engineering techniques used by cybercriminals to try to trick users into giving away their personal data. The unit will look at the more common cybercrimes such as hacking, DDoS attacks, and malware, as well as looking at methods to protect ourselves and our networks against these attacks.

GCSE Computer Science

Year 10 - Unit-5-Impacts-of-digital-technology –

Discuss the impacts of digital technology on the wider society including ethical issues, cultural issues and environmental issues

- Discuss the impact of digital technology regarding legal issues and privacy issues
- Describe legislation relevant to Computer Science including
 - The Data Protection Act 2018
 - Computer Misuse Act 1990
 - Copyright Designs and Patents Act 1988

Year 11 will revisit Unit 5 as part of their revision package

A level Computer Science

KS5 – Year 12 - 1.5.2 Ethical and Moral Issues in CS

Discuss the impacts of digital technology on the wider society including ethical issues, cultural issues and environmental issues

- Discuss the impact of digital technology regarding legal issues and privacy issues
- Describe legislation relevant to Computer Science including
 - The Data Protection Act 2018
 - Computer Misuse Act 1990
 - Copyright Designs and Patents Act 1988

Then reviewed for revision in Year 13

Education – parents / carers

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website
- Parents / Carers evenings / sessions
- High profile events / campaigns eg Safer Internet Day
- Reference to the relevant web sites / publications eg www.swgfl.org.uk
www.saferinternet.org.uk/ <http://www.childnet.com/parents-and-carers>

Education & Training – Staff / Volunteers

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

- A annual programme of formal online safety training will be made available to staff. This is compulsory to complete This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school policy and Acceptable User Agreements.
- The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days as appropriate.
- The DSL will provide advice / guidance / training to individuals as required.

Training – Directors and Governors

It is compulsory for Directors and Governors to take part in online safety training / awareness sessions, and this may be offered in a number of ways:

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

Email

E-mail is an essential means of communication for both staff and pupils. Directed e- mail use can bring significant educational benefits and interesting projects. However, un-regulated e-mail can provide a means of access to a pupil that bypasses the traditional academy boundaries. In the school context, therefore, e-mail is not considered private and is monitored by staff, whilst trying to achieve a balance between monitoring that is necessary to maintain the safety of pupils and the preservation of human rights, both of which are covered by recent legislation.

Pupils

- Pupils will only use approved e-mail accounts on the school system where contacts have been made and approved between organisations such as partner schools. Pupils may not access personal email accounts in school.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

Staff

- Email sent to an external organisations containing personal information must be password protected.
- Internal emails should use pupil's initials where appropriate.
- Staff must be familiar with the Code of Conduct and never use their personal email or social media accounts to conduct school business or contact a child

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying 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:

- When using digital images, staff should inform and educate pupils 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must delete any images of pupils within a week. This should allow time for staff to use images of pupils to create Assessment journals using such Apps 'Pic Collage'. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere (including Youtube) that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs or videos of pupils are published on the school website or Youtube.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018, UK GDPR and the Trust's Data Protection Policy.

An annual programme of data protection training will be made available to staff. New staff should receive a data protection induction within their first month of employment.

Communications

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:

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

- The official academy email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the academy policy, 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.
- Any digital communication between staff and parents / carers must be professional in tone and content. These communications may only take place on official (monitored) academy systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class email addresses will be provided for educational use.
- Pupils 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.
- Personal information should not be posted on the academy website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools/academies and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the academy or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

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

- Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions

School staff should ensure that:

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

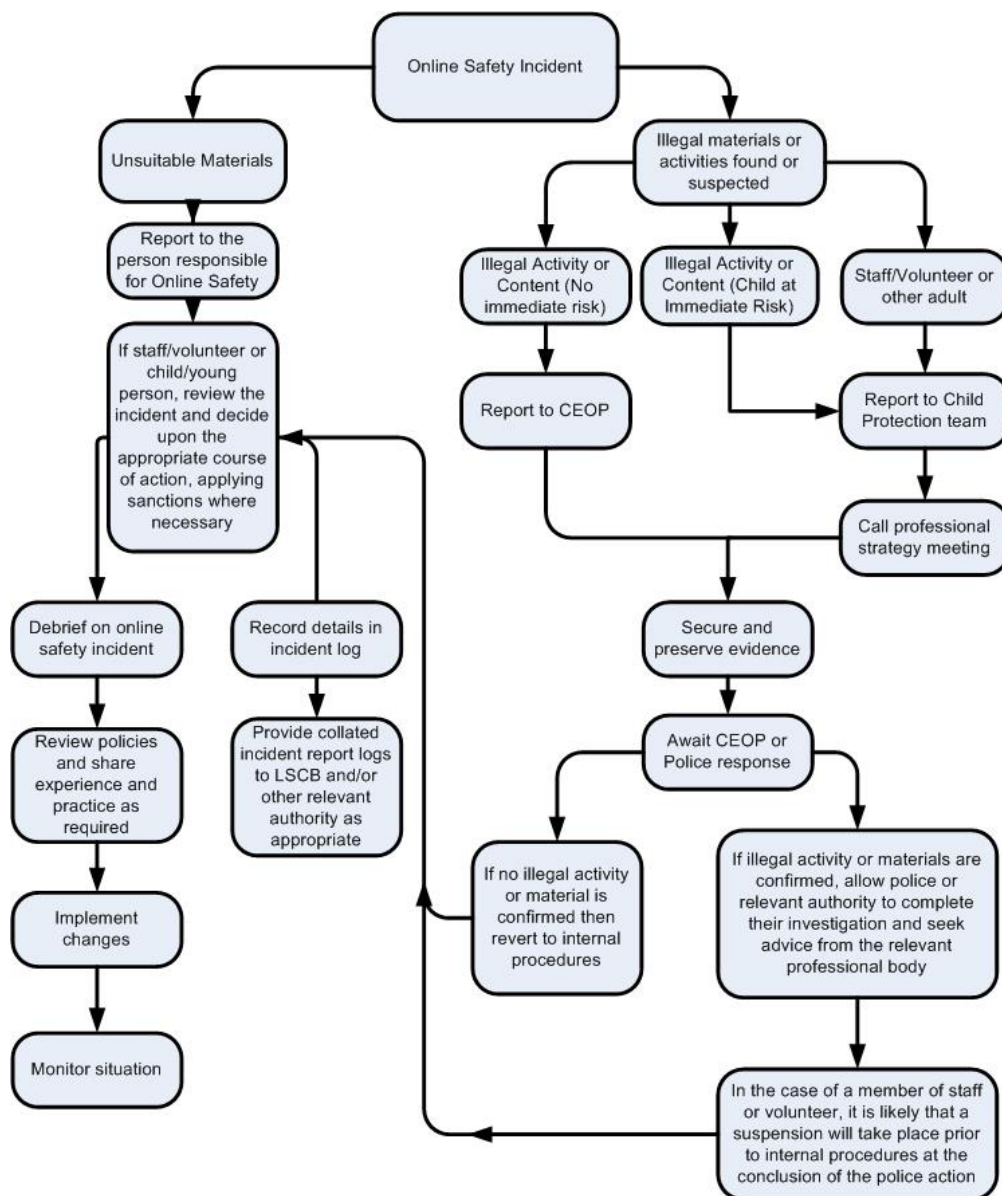
The academy's use of social media for professional purposes will be checked regularly by the Headteacher and e-safety officer to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Responding to incidents of misuse

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 (see "User Actions" above).

Illegal Incidents

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



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow academy policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.

- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the academy and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes. Any searches should be completed in line with 'Searching, Screening and Confiscation Advice for Schools 2022'

Reviewed by:	V Shelley R Mushing	April 2024 September 2024
Senior Lead Review:	R Darling	February 2025
Next Review Date:		April 2026
Approved by Directors:		24 March 2025

Signed:



Lois Whitehouse
CEO



Nicky Aston
Chair of Standards