ICT and Online Safety Policy

Approved by Governors Safeguarding Committee on 24th March 2025

Review date: Spring 2026

Responsible for review: Digital Lead/ DSL

Published on website: Yes

Contents

Summary of Changes (shown in red):

*Policy aims to reflect the importance of AI and its growing role within the school community.
*Responsibilities assigned to reflect the need to align with Safeguarding priorities and to be compliant with Data security protocols.
*Learners will receive a greater education in AI literacy and warned of its attendant risks.
*Staff & Learners alike will have a revised Acceptable Use Policy to agree to.

1. Aims

- To empower the school community based on an understanding of risk categories pertinent to online safety
- To have clear processes in place for hardware & software use by all pupils, staff, volunteers and governors.
- To ensure all stakeholders are aware of their responsibilities in identifying, intervening and escalating an incident where appropriate.
- To promote the ethical, responsible, and safe use of AI and emerging digital technologies within the school community by providing guidance on their appropriate use, addressing potential risks and benefits, and establishing procedures to manage concerns related to AI-generated content and misinformation.

2. Legislation

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Categories of Risk

The 4 key categories of risk which underpin the policy are:

- Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism. This also includes AI-generated content risks, such as deepfake videos, AI-generated misinformation, and manipulated media that spread false narratives or deceptive information.

- Contact – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- Conduct – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scam**s**

4. Roles and responsibilities

The governing body will:

- Take overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- Coordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)

The Headteacher will:

- Oversee the activities of the designated safeguarding lead and ensure that the DSL responsibilities listed in the section below are being followed and fully supported
- Ensure that policies and procedures are followed by all staff
- Ensure that AI technologies used in school align with safeguarding policies, data protection laws, and ethical guidelines.

Designated Safeguarding Lead will:

- Carry out duties which are set out in our child protection and safeguarding policy as well as relevant job descriptions.
- Take lead responsibility for online safety in school, in particular:
- Support the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Work with the Headteacher, Network manager and Digital Lead, as necessary, to address any online safety issues or incidents
- Manage online safety issues and incidents in line with the school child protection policy

- Ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Update and delivering any relevant staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Provide reports on online safety in school to the headteacher and/or governing board
- (This list is not intended to be exhaustive)

The Network manager will

- Put in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conduct a full security check and monitoring the school's ICT systems on a weekly basis
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensure that any online safety incidents are logged (see appendix 5) and the information disseminated to the DSL
- (This list is not intended to be exhaustive)

Digital Lead will

- Ensure AI initiatives are compliant with safeguarding and data security policies.
- Provide guidance on AI literacy and responsible AI use for students and staff.
- Have oversight of ICT strategy and operations and Line Manage the Network Manager.
- Oversee curriculum content and thus liaise with PD & Computing Lead to ensure their responsibility for online safety is delivered.
- (This list is not intended to be exhaustive)

All staff will

- Maintain an understanding of this policy and implement it consistently
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Work with the DSL to ensure that any online safety incidents are logged (see appendix 5) so that the policy can be implemented
- Ensure that any incidents of cyber-bullying are are logged (see appendix 5) so that the policy can be implemented
- Ensure that AI tools used in teaching and learning align with the school's policies on data security and ethical use.

- Monitor AI usage in student assignments to prevent overreliance on AI-generated content and ensure academic integrity.
- (This list is not intended to be exhaustive)

Personal Development Lead will

- Deliver on the key responsibilities from DfE as of September 2019 for September 2020 (below taken from DfE press release on 19 July 2018 on New relationships and health education in schools):

- Embed consent, mental wellbeing, healthy relationships and staying safe online into the SMSC / RE curriculum, "complementing the existing computing curriculum – and how to use technology safely, responsibly and respectfully. Lessons will also cover how to keep personal information private, and help young people navigate the virtual world, challenge harmful content and balance online and offline worlds."
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within PD/RE

Computing Lead will

- Deliver on the key responsibilities from online safety elements of the Computing curriculum in accordance with the national curriculum
- Work closely with the DSL and all other staff to ensure an understanding of the issues, approaches and messaging within Computing
- Collaborate with technical staff and others responsible for ICT use in school to ensure a common and consistent approach, in line with acceptable-use agreements

Parents will

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)
- Seek further guidance on keeping children safe online from the following organisations and websites, if they would like more information:
    1. What are the issues? – UK Safer Internet Centre
    2. Hot topics – Childnet International
    3. Parent resource sheet – Childnet International
    4. Healthy relationships – Disrespect Nobody

5. Educating Students

Pupils will be taught about online safety as part of the curriculum;

In Key Stage 3, pupils will be taught to:

- Understand 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

Pupils in Key Stage 4 will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the end of secondary school, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
- Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.
- Through AI Education, learners will be educated on how to safely use AI programs as a teaching tool. They will also be informed about the ethical implications of using AI-generated text and images in coursework and assessments.

6. Handling online-safety concerns and incidents

It is vital that all staff recognise that online-safety is a part of safeguarding (as well as being a curriculum strand of Computing and Personal Development (from September 2019 for September 2020) the new statutory Health Education and Relationships Education (for secondaries: Relationships and Sex Education). General concerns must be handled in the same way as any other safeguarding concern. A further dimension to this was in the latest statutory guidance from KCSIE (here) which specified the need to put in place filtering and monitoring mechanisms so as to assess likely risk categories from all usage within our domain. This is subject to triage by the safeguarding team from a network manager report via securus software. The safeguarding team allocates staff to follow up;

- Subject teachers for items looked at during ICT lessons
- Year teams for inappropriate items looked at on chromebooks
- Safeguarding team follows up serious concerns like PREVENT and suicide

Actions are then logged on the report. Any safeguarding concerns that persist are followed up in the normal manner by the safeguarding team.

7. Searching and confiscation

In line with the DfE guidance 'Searching, screening and confiscation: advice for schools', the Headteacher and staff authorised by them have a statutory power to search pupils/property on school premises. This includes the content of mobile phones and other devices, for example as a result of a reasonable suspicion that a device contains illegal or undesirable material, including but not exclusive to sexual images, pornography, violence or bullying.

8. Misuse of school technology (devices, systems, networks or platforms)

Clear and well communicated rules and procedures are essential to govern pupil and adult use of school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school). Where pupils contravene these rules, the school behaviour policy will be applied; where staff contravene these rules, action will be taken as outlined in the staff code of conduct/handbook. Further to these steps, the school reserves the right to withdraw – temporarily or permanently – any or all access to such technology, or the right to bring devices onto school property.

Misuse of AI tools, such as deepfake technology, AI chatbots for generating inappropriate content, or AI-powered plagiarism, will be treated as a breach of the school's ICT policy. Using AI-generated text or code without proper attribution in assignments will be considered academic misconduct.

9. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use where relevant.

10. Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use.
- The school is not responsible for the loss, damage or theft of any personal mobile device
- Sixth Formers should only use mobile devices in the Sixth Form block
- The sending of inappropriate text messages between any member of the school community is not allowed
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device

11. Servers

Servers are kept in a locked and secure environment and permission must be sought before any image or sound recordings are made on these devices of any member of the school community as only designated staff are allowed access. Back up tapes are encrypted by appropriate software and are made regularly and are securely stored in a fireproof container

12. Disposal of Redundant ICT Equipment

ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data. Disposal of any ICT equipment will conform to: The Waste Electrical and Electronic Equipment Regulations as well a the data protection Act: http://www.ico.gov.uk/what_we_cover/data_protection.aspx

13. Breaches

A breach or suspected breach of policy by a school employee, contractor or learner may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure. Policy breaches may also lead to criminal or civil proceedings.

14. Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Network Manager.

15. Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. Information can be accessed on http://www.ico.gov.uk/for_organisations/data_protection/security_measures.aspx

- The school gives relevant staff access to its SIMS, with a unique username and password
- It is the responsibility of everyone to keep passwords secure. It is recommended that passwords are changed regularly
- Staff are aware of their responsibility when accessing school data
- Staff must not give learners access to computers using staff login details
- Staff have been issued with the relevant guidance documents and the protocol for ICT Acceptable Use (**see Appendix C**)
- The Headteacher is responsible for deciding levels of access to school data.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed.

Appendix A

Suspected Indecent Imagery Protocol

'Indecent' is not defined in legislation. For most purposes, if imagery (moving or still) contains a naked young person, a topless girl, and/or displays genitals or sex acts, including masturbation, then it will be considered indecent. Indecent images may also include overtly sexual images of young people in their underwear.

Confiscate it	Close it down	Report it

ALL STAFF

If the imagery has been shared across a **personal mobile device**:

Always..

- Confiscate and secure the device(s)
- Inform any DSL

Never...

- View the imagery (if viewed accidentally always report this)
- Send, share or save the image anywhere
- Allow students to do any of the above once you know about the imagery
- Delete the imagery unless directed to do so by the DSL

If the imagery has been shared across a **school network, a website or a social network**:

Always..

- Block the network to all users and isolate the imagery
- Inform the DSL

Never...

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in your safeguarding and child protection policies and procedures.
- Delete the imagery unless directed to do so by the DSL

Additionally never..

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem
- Print out any material for evidence
- Move any material from one storage device to another

DSL ACTIONS

The DSL will conduct the investigations after they have been made aware of the concern. Full notes will be kept in a learner safeguarding file. The purpose of the investigation is to:

- Identify, without looking, what the image contains and whether anyone else has been involved.

- Find out who has seen or shared the image and how further distribution can be prevented.

They will involve parents, social services or the police where necessary

The DSL may immediately refer to police and/or children's social care if:

- The incident involves an adult
- There is reason to believe that a young person has been coerced, blackmailed or groomed, or if there are concerns about their capacity to consent (for example, owing to special educational needs)
- What you know about the imagery suggests the content depicts sexual acts which are unusual for the young person's developmental stage, or are violent
- The imagery involves sexual acts and any pupil in the imagery is under 13
- You have reason to believe a young person is at immediate risk of harm owing to the sharing of the imagery, for example, the young person is presenting as suicidal or self-harming

Appendix B

Learner Acceptable Use Agreement

- I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network, other systems and resources with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with learners, staff or others are responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will not take Images of anyone at school.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, learners or others distress or bring into disrepute.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community
- I will use AI tools responsibly and will not rely on them for completing assignments dishonestly.
- I understand that AI-generated information may be inaccurate or biased, and I will critically evaluate AI-generated content.
- I will not use AI to impersonate others, create deceptive content, or engage in cyberbullying.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.

Appendix C

Acceptable Use Agreement Staff, Governors, Visitors & Volunteers

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This Agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. Please read the Code of Conduct.

I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.

- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour which I believe may be inappropriate or concerning in any way to the Designated Safeguarding Lead (if by a learner) or Headteacher (if by an adult).
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with learners and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to learners.
- I will only use the approved, secure e-mail system(s) for any school business.
- will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted (ask for help with setting up passwords)
- I will not install any hardware or software.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of learners and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset any member of the school community.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help learners to be safe and responsible in their use of ICT and related technologies.

- I will comply with the school's communication protocols
- I will use AI tools ethically and ensure students understand the risks of AI-generated content.
- I will verify AI-generated information before using it in educational materials or assessments.
- I will ensure that AI use in teaching aligns with academic integrity and safeguarding policies.

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT at school & home

Signature …….…….…… Date ……

Full Name …….....(printed)

Appendix D

Code of Conduct

Communication between pupils and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, emails, digital cameras, videos, web-cams, websites and blogs. Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role. If a pupil seeks to establish social contact, or if this occurs coincidentally, the adult report the contact to a Senior Leader and not engage in ongoing communication.

Staff and volunteers must not give their personal contact details such as home/mobile phone number; home or personal e-mail address or social networking details to pupils. It is recommended that staff ensure that all possible privacy settings are activated to prevent students from making contact on personal profiles and to prevent students from accessing photo albums or other personal information which may appear on social networking sites. If staff encounter pupils through common membership of off-site organisations they are reminded to consider their professional obligations and also to familiarise themselves with the Child Protection Policy of the other organisation

Computers – Staff will be issued with a password to access the academy Intranet and the internet. Staff are responsible for the use of any laptop provided to them for the better performance of their duties and should therefore be careful about who has access to their password and machine.

Mobile Phones – Staff should not use their mobile phones during lessons and should not make or receive calls at any time that they supervise students, unless in an emergency situation.

All usage of electronic equipment must be in accordance with the school's Acceptable Use Policy.
Other equipment – Any items belonging to the Academy must remain available to be used by staff and students as necessary. Staff will be responsible for the safekeeping of equipment loaned to them by the Academy.

Personal property of a sexually explicit nature such as books, magazines, CDs, DVDs or such material on any electronic media must not be brought onto or stored on the school premises or on any school equipment.

Social networking sites and blogging are popular. Staff, governors and volunteers must not post material which damages the reputation of the school or which causes concern about their suitability to work with children and young people. Those who post material which may be considered as inappropriate could render themselves vulnerable to criticism or allegations of misconduct which may be dealt with under the school's disciplinary procedure.

Under no circumstances should adults access inappropriate images in school or on school equipment outside school. Deliberately accessing pornography on school equipment will be treated as gross misconduct and may be a criminal offence. Accessing indecent images of children on the internet, and making, storing or disseminating such material, is illegal and is likely to lead to criminal prosecution and may result in barring from work with children and young people.