ICT & Online Safety Policy

2023-24

Contents

1. Aims

This policy aims to promote a safe and secure digital environment and encourage positive behaviours for all members of our school community. It is designed to ensure compliance with relevant UK legislation, and has been prepared with reference to the statutory guidance from the Department for Education's Keeping children safe in education 2023 (KCSiE 2023).

Specifically, this policy will help:

- Safeguard students and staff when using devices and online technologies, both on and off the school premises
- Promote the safe and responsible use of devices and online technologies
- Provide clear guidelines on appropriate online behaviour for students and staff including any sanctions that may result in the event there are infringements
- Raise awareness of both persistent and trending digital and online safety risks
- Provide mechanisms for easily reporting and addressing online safety concerns

This policy should be understood in the context of other relevant school policies and procedures, especially the school Safeguarding Child Protection Policy, Behaviour and Discipline Policy, Anti-Bullying Policy, staff Code of Conduct, The Staff ICT Acceptable Use Agreement and the Student ICT Acceptable Use Agreement. It reflects the provisions in the school's Safeguarding Child Protection Policy related to online behaviours and includes commitments for the appropriate filtering and monitoring on school managed devices and systems.

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping children safe in education 2023, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- 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 students' electronic devices where they believe there is a 'good reason' to do so.

This policy applies to all members of the school community including staff, students, volunteers, parents/guardians, directors/governors and visitors. That is, anyone who uses the school ICT systems, services or devices; on or off the school premises; including anyone accessing the school's ICT systems or services from non-school owned devices.

The Education and Inspections Act 2006 empowers Heads to such extent as is reasonable, to regulate the behaviour of students when they are off school site and empowers staff to impose disciplinary penalties for inappropriate behaviour. This is relevant to incidents of child-on-child abuse such as cyberbullying, and other online safety issues covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers in regard to searching for, and of, electronic devices and the deletion of offending data. In the case of both acts, action can only be taken over issues covered by the school's Safeguarding Child Protection, Child-on-Child Abuse and Behaviour Policies. The school will deal with such incidents within the scope of these policies and will, where known, inform parents/guardians of incidents of inappropriate online behaviour that take place out of school. The school also has responsibilities under the Counter Terrorism and Security Act (2015), commonly known as the Prevent Duty and measures in this policy are aligned with this.

Categories of Online Risks

KCSiE 2023 outlines four high level areas of online safety risk. Most safeguarding risks present in the physical world can extend into the digital world and become amplified online. In response:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism. The school employs appropriate filtering systems that are regularly updated with threat intelligence to prevent access to illegal, inappropriate, or harmful content and monitoring systems that alerts relevant staff of behaviours that may be putting children at risk. **This is regulated by the IWF (Internet Watch Foundation)**.
- **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. Measures are in place to monitor and minimise harmful online interactions including child-on-child risks such as cyberbullying, the sharing of explicit images and peer pressure; as well as risks typically posed by adults such as online grooming and radicalisation.
- **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. The school teaches students and staff about responsible online behaviour, and highlights the risks, for example, of sharing explicit images, or engaging in online trolling, harassment or bullying.

- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams. Online safety learning will include age-appropriate content covering risks such as those posed by the inappropriate sharing of personal data or images; engaging with in-game purchases, online gambling or online scams; and infringing others' intellectual property.

As a consequence of the rapid pace of i) new technologies being made available at low cost, and ii) development in online social and cultural trends, new risks and harms emerge quickly. To address this the school adopts a school wide approach that annually:

- Delivers up to date digital and online safety learning as part of the ICT curriculum and has a whole school approach that integrates learning opportunities across the curriculum
- Provides up to date ICT and online safety training (including cyber security & data protection) to all staff
- Assesses the provisions in place for filtering and monitoring of online content and the processes for managing and reporting of alerts and infringements
- Reviews technology, social and online trends to ensure the school's policies & procedures, technical measures, training, and curriculum are updated to reflect the current risks most pertinent to students, staff and the wider school community.

The current IT and online risk landscape

The following risks are considered current and most pertinent to students, staff and our wider school community:

- Online hate, misogyny, violence, conspiracy, fake news and the spreading of false information
- Cyberbullying, especially on personal messaging apps and in-game chat
- Health and well-being as a result of the amount of time spent online / gaming
- Inappropriate disclosure (and use) of personal information
- Sending, receiving or using of personal images or data (including that of a sexual nature)
- Lack of care or consideration for the personal data and/or intellectual property of others
- Not verifying the authenticity or accuracy of online content
- Ignorance of one's digital footprint and online reputation
- Online grooming
- Hijacking of accounts or impersonating another person, devices and data including identity theft via email phishing campaigns or through compromised or spoof websites and online services including using someone else's digital identity
- Risk of radicalisation and/or access to online content that may lead to indoctrination into any form of extreme ideology
- Risk of AI generated video, audio, images or text that is intended to deceive, defraud or elicit a reactive response

3. Roles and responsibilities

3.1 The headteacher and senior leaders

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.2 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputy designated leads (DDSL's) are set out in our child protection and safeguarding policy.

The designated Child Exploitation and Online Protection Officer (CEOP Officer) takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher and other senior leaders in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the senior leadership team to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Working with the ICT providers to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT provider and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and organisation (as appropriate) Takes the lead responsibility for all digital and online safety issues across the school
- Has the primary role in preparing updating and reviewing this ICT & Online Safety Policy; the staff and the student Acceptable Use Agreements.
- Ensures that all students are aware of the expectations documented in the Students Acceptable Use Agreement and maintains the records of student (and parental) agreement to them
- Is responsible for organising and delivering digital and online safety training as well as providing advice to staff, children and parents on these matters
- Make sure all staff have reviewed this ICT & Online Safety Policy and the Staff ICT Acceptable Use Policy and with the support of HR maintains the records of agreement to them
- Ensures that all children are taught how to keep themselves and others safe when using technology and online

- Demonstrates leadership in the schools commitment to keep current the digital and online safety learning content, and that it is a running and interrelated theme across the curriculum and part of the whole school approach to safeguarding
- Liaises with the school IT team to ensure that filtering and monitoring is working effectively without overblocking and on all other relevant digital and online safety and cyber security matters
- Acts as a primary liaison for all digital and online safety concerns raised by students, staff and any other member of the school community
- Communicates regularly with, SLT and the DSL and deputies to discuss current issues and trends
- Keeps current with digital and online trends, the safety issues associated with them and updates to relevant legislation, especially that which relates to the safeguarding of children
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

3.3 The ICT provider

The ICT provider is responsible for:

- Are responsible for the running, maintenance & updates of filtering, monitoring and alerting systems in line with their escalation policy
- Taking a lead role in the periodic review of the technical provision for filtering and monitoring and a supporting role in the regular review of the current digital and online safety risk landscape
- Provide assistance to the DSL and deputies, SLT when investigating digital and online safety incidents, including event logs analysis and digital evidence gathering
- Provide strategic advice on appropriate technologies to ensure the school upholds its digital and online safety obligations
- Keep current with technologies and industry trends related to digital and online safety, cyber-security and data security
- Ensure the school network and systems are appropriately monitored in order that any misuse or attempted misuse can be identified and investigated
- Maintain frequent backups of critical data (at least daily) and systems (at least weekly), that encrypted copies of these are stored securely in more than one location, are locked to prevent accidental or malicious corruption and recovery routines are tested routinely in order that critical data and systems can be recovered in a timely fashion when required
- Makes sure all staff member's access to school systems is secured with unique credentials and protection is further enhanced by emails with multi-factor authentication (MFA) wherever possible
- Deploy and maintain and monitor an end-point detection and response (EDR) system on all managed devices (Intune)

- Patch and maintain systems and software ensuring all patches rated as "critical" are installed with 7-14 days of release
- Configure and maintain a strong email security stance to protect against phishing and email borne threats
- Manage, maintain and monitor a secure gateway(s) between the school private network(s) and the internet

3.4 All staff, volunteers and visitors

All staff, volunteers and visitors are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Demonstrate good digital and online safety behaviours throughout all areas of practice
- Liaise with the DSL to incorporate digital and online safety learning into their curriculum / lesson plans and always take opportunities to include online safety learning points wherever appropriate
- Guide and supervise students with care when engaging in digital and online activities and be alert to the risks and harms that may present
- Help students build critical research skills by cross referencing sources, disregarding fake news and false information and help develop awareness of the legal issues relating to digital content such as copyright laws and plagiarism
- Teach children to keep themselves safe, including online and when accessing remote learning.
- Take responsibility for checking online content before using in class and reporting all instances where inappropriate content gets through the web filter
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that students follow the school's terms on acceptable use
    - Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by immediately completing an incident report using our Safeguarding software (CPOMS)
- Following the correct procedures by contacting the ICT provider and requesting access to specific and named educational material if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the CEOP Officer and DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

Further, all staff should be aware that technology is a significant component in many safeguarding and wellbeing cases. Children are at risk of abuse online as well as in person. In many cases abuse 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.

3.5 Students

All students are responsible for:

- Be open to learn about and adopt good digital and online safety practices and show this in how you use technology and online both in and out of school
- Be kind and mindful of your own and others safety when using devices and when online
- Always tell your teacher or trusted member of school staff straight away if you know of, see or receive digital or online content that makes you feel unhappy, worried or vulnerable
- Students will receive a copy of the ICT and online Acceptable use Agreements. They are expected to sign to say they understand the content

3.6 Parents/carers

Parents/carers are expected to:

- 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 (Held in the Admissions Pack)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

4. Educating students about online safety

Students will be taught about online safety as part of the ICT and Personal Development curriculum. The theme of friendships and relationships is also covered through our thematic World Around Us curriculum.

As part of these curriculum areas, students;

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

- Know their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Learn 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
- Understand not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- Know what to do and where to get support to report material or manage issues online
- Understand the impact of viewing harmful content
- Know 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
- Know that sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- Learn how information and data is generated, collected, shared and used online
- Learn 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

5. Cyber-bullying

5.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

5.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the headteacher. In the absence of the headteacher, they will seek advice from the DSL or DDSL.
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, but is not deemed to cause harm, undermine the safe environment of the school or commit an offence the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The student and/or the parent/carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's

latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

5.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Edison Pace School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

6. Acceptable use of the internet in school

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.

7. Students using mobile devices in school

Students may bring mobile devices into school, but must hand them in immediately on arrival where it will be placed inside a locker.

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

8. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour and/or bullying policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the terms of the Acceptable Use Policy and the Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

All new staff members will receive training, as part of their induction, and will be asked to complete an Acceptable Use Policy.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and DDSL will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

More information about safeguarding training is set out in our child protection and safeguarding policy.

10. Filtering and monitoring arrangements

- The school has appropriate filtering and monitoring systems in place and reviews their effectiveness each year.
- The leadership team and relevant staff have an awareness and understanding of the provisions in place for filtering and monitoring and ensure that they are managed effectively
- There is a process in place for escalating and dealing with concerns about filtering and monitoring systems themselves. In all cases, concerns should be first addressed to the DSL (or a deputy), whether there is, or is not, an immediate concern for the wellbeing of a child or other person. The DSL or a deputy will involve the IT team in order to address the concerns raised.
- The school has taken into consideration the number of and age range of children (including those who are potentially at greater risk of harm) and how often they access school digital and online systems and have implemented filtering and monitoring solution(s) that on balance, mitigate against the safeguarding risks. We will reassess this provision on an annual basis

Further, in line with the DfEs Filtering & Monitoring Standards, this school:

- Has assigned roles and responsibilities to manage filtering and monitoring:
    - the IT team are responsible for the setup, maintenance and management of the systems, including liaising with technology suppliers, and play a supporting role in responding to alerts
    - the DSL take the lead role in responding to filtering and monitoring alerts, regularly reporting trends to SLT and liaising with the IT team to ensure the systems are working effectively
    - In addition, the DSL and the IT Team will investigate all concerns raised about the schools filtering and monitoring systems
- Always aims to block harmful and inappropriate content without unreasonably impacting teaching and learning
- Has monitoring strategies in place to help meet our safeguarding responsibilities. These include physical monitoring by teachers and pastoral support watching the screens of students, monitoring of network traffic and online activities and monitoring of activity on school managed devices

11. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure