Kirtlington
C.E. School

Online Safety and Acceptable Use Policy

Reviewed and approved by: FGB

Policy Reviewed: April 2026

Future Review: April 2027

Scope of the Policy

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

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

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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

Content – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism

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 scams

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school.

Governors:

Governors are responsible for the approval of the E-Safety Acceptable Use Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. The Safeguarding member of the Governing Body has the role of E-Safety Governor. The role of the E-Safety Governor will include:

- regular meetings with the headteacher:
- regular monitoring of e-safety incident logs

- reporting to relevant Governors

The school will monitor the impact of the policy using:

- Logs of reported incidents on CPOMS
- Filtering and monitoring software logs
- Notification of inappropriate content being accessed via 123ICT
- Surveys / questionnaires of
  - pupils
  - parents / carers
  - staff

Headteacher and Senior Leaders:

- The Headteacher has a duty of care for ensuring the safety (including e-safety) of members of the school community.
- The Headteacher and another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff. (see flow chart on dealing with e-safety incidents – included in a later section – "Responding to incidents of misuse" and relevant Local Authority HR / other relevant body disciplinary procedures).
- The Headteacher is responsible for ensuring that staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- Takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- Liaises with the Local Authority / relevant body
- Liaises with school technical staff
- Receives reports of e-safety incidents.

The ICT Leader:

- Liaises with school technical staff as required
- meets regularly with ICT/E-Safety Governor to discuss current issues
- attends relevant meetings
- reports when appropriate to Senior Leadership Team
- Provides training and advice for staff on internet safety

Network Manager / Technical staff: 123ICT

The Network Manager / Technical Staff is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority E- Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed for Staff and visitors
- filtering and monitoring is applied and reviewed
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet / Virtual Learning Environment / remote

access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and E-Safety Coordinator for investigation, action and sanction

- that monitoring systems are implemented and updated as agreed in school policies

Teaching and Support Staff are responsible for ensuring that:

- they have an up-to-date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed to say they understand the E-safety Acceptable Use Policy
- they report any suspected misuse or problem to the Headteacher for investigation / action / sanction
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
  all staff are familiar with the Project Evolve scheme of work used explicitly to teach on-line safety.
- pupils understand and follow the e-safety and acceptable use policy / agreements
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) 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 / Safeguarding Designated Person: Kyla Bates and Victoria Grocutt, should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- online radicalisation
- cyber-bullying

Children:

- are responsible for using the school digital technology systems in accordance with the ICT Acceptable Use Policy
- have a good understanding of research skills
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand school procedure on the use of mobile devices and cameras. They should know that their personal mobile devices or tablets are not permitted in school. Children in Y5/6 with permission to have a mobile telephone for the journey to/from school must hand these in to their class teacher on arrival. If any unauthorised device is brought to school, it should immediately be taken to the school administrator to store securely in the office until the end of the school day, and reported to parents.
- Children are taught about safe use of images and cyber-bullying out of school and

realise that the school's E-Safety Acceptable Use Policy covers their actions out of school, if related to their membership of the school

Parents / Carers
The school will take every opportunity to help parents understand the need to use the internet / mobile devices in an appropriate way through parents' evenings, newsletters, letters and website. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to on-line student / pupil records
- their children's personal devices in the school

Community Users
Community Users who access school systems / website as part of the wider school provision will be expected to sign an internet usage agreement.

Policy Statements

Education –children
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 e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety is taught as a discrete subject and is also a focus in all areas of the curriculum. The e-safety curriculum is broad, up-to-date, provides progression, assessment:

- A planned e-safety curriculum (Project Evolve) is provided in addition to the computing curriculum (Teach Computing).
- Key e-safety messages are reinforced during the day through other activities
- Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information.
- Pupils should be helped to understand the need and be 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 and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Education – parents / carers
Some parents and carers may not have a full understanding of online safety risks, even though they play a vital role in supporting their children's learning and in overseeing their online activity. They may also be unaware of how frequently children and young people encounter potentially harmful or inappropriate material online and may feel uncertain about how best to respond.

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

- Letters, newsletters, web site
- Parents sessions on e-safety
- High profile events / campaigns e.g. Safer Internet Day

Education and Training – Staff / Volunteers

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

- A planned programme of formal e-safety training will be made available to staff by 123ICT. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly**.**
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- The ICT leader will receive updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This ICT policy and its updates will be presented to and discussed by staff in staff meetings and INSET days.

Training – Governors

Governors should take part in e-safety training (training programme notified by 123ICT), with particular importance for those who are members of any sub-committee involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the school and feed back to the governing body.
- Participation in school training / information sessions for staff or parents

Technical – infrastructure / equipment, filtering and monitoring

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

- There will be regular reviews and audits of the safety and security of school technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to School technical systems and devices.
- All users will be provided with a username by the 123ICT who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username.
- 123ICT is 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. Content lists are regularly updated. There is a clear process in place to deal with requests for filtering changes.
- The school has provided enhanced / differentiated user-level filtering
- 123ICT regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person. Pupils to report incidents to their teachers and teachers report to 123ICT
- 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. These are tested regularly by 123ICT. The school infrastructure and individual workstations have updated firewalls.
- An agreed policy is in place for the provision of temporary access of “guests” (eg

trainee teachers, supply teachers, visitors) onto the school systems. Visitors are to sign and agree to the internet usage agreement and are limited to the children's level of access.

- An agreed policy is in place regarding the extent of personal use that staff are allowed on school devices that may be used out of school in accordance with the school's code of conduct.
- Removable media (eg memory sticks / CDs / DVDs) is only used in exceptional circumstances on school devices. Personal data cannot be sent over the internet or taken off the school site.

Bring Your Own Device (BYOD)

- These devices are covered by the school's normal filtering systems, while being used on the premises

Use of digital and video images

The school will inform and educate users about risks relating to images and videos 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 e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers may be able to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be 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 follow school policies concerning the sharing, distribution and publication of those images.
- 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 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 of pupils are published on the school website.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council enforced in Spring 2018, which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure

- Only transferred to others with adequate protection.

The School must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible person is appointed / identified - Data Protection Officer
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

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 School 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 School 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 pupils or parents / carers (email, chat, VLE etc.) must be professional in tone and content. These communications may

only take place on official (monitored) School systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Whole class / group email addresses may be used at KS1, while pupils at KS2 will be provided with individual School email addresses for educational use.
- Pupils are taught about e-safety issues, such as the risks attached to the sharing of personal details. They are also taught strategies to deal with inappropriate communications and are reminded of the need to communicate appropriately when using digital technologies.
- Personal information is not posted on the School website and only official email addresses are 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 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 School 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 as defined in the Child Protection and Safeguarding policy.
- Risk assessment, including legal risk

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 school or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Artificial intelligence (AI)

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

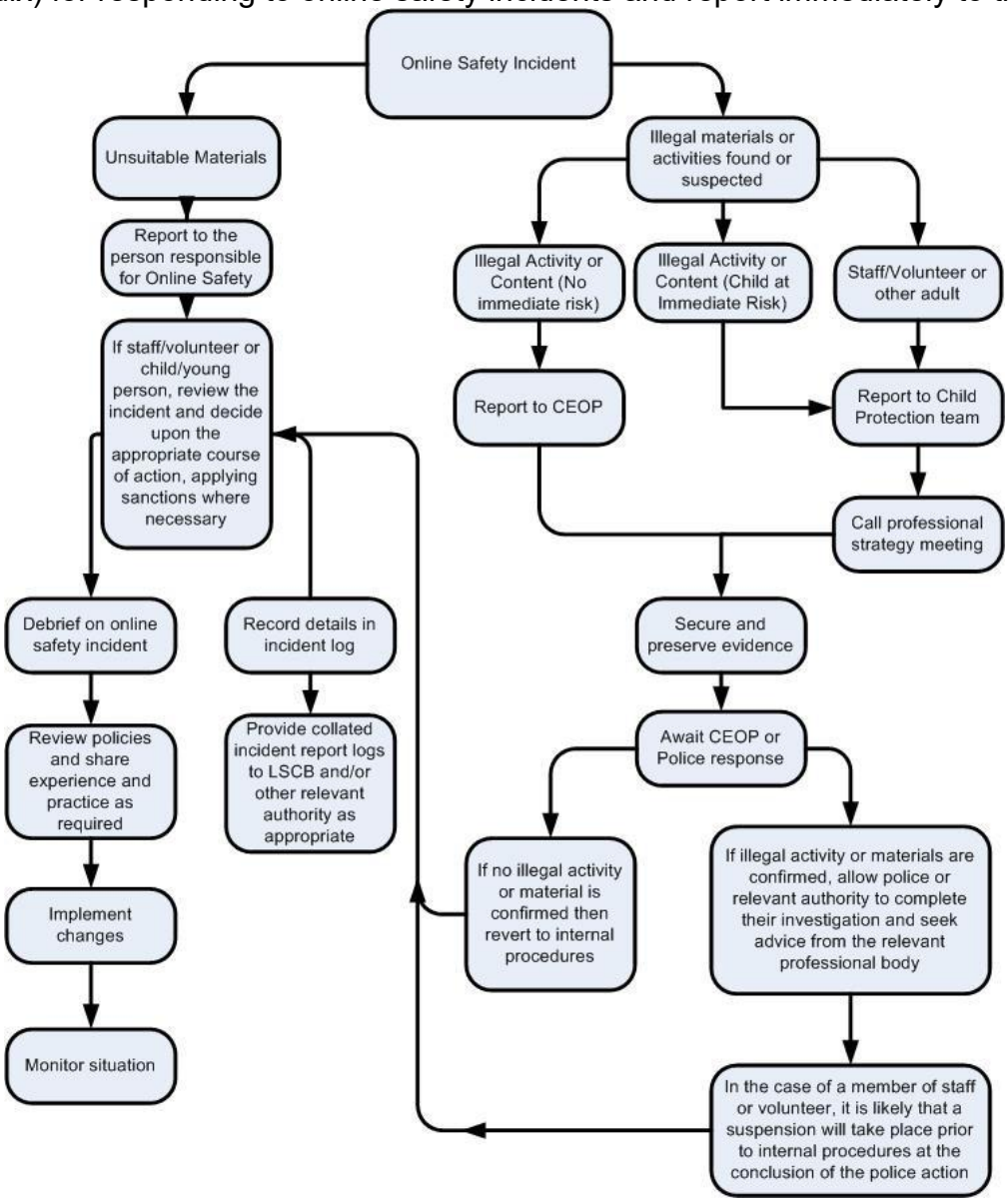
Kirtlington School recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Kirtlington will treat any use of AI to bully pupils very seriously, in line with our anti-bullying policy.

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 by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by it, including, but not limited to, pupils and staff.

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.

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 School 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 school 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.

School Actions & Sanctions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Associated policies

Anti-bullying policy, codes of conduct, disciplinary policy, data protection policy, mobile phone and smart devices policy, restorative practice and behaviour policy, social media policy and safeguarding policy.