



e-Safety Policy

Reviewed: September 2025

Next Review: September 2026

Responsible: Mr Zubair Kola

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Surveys/questionnaires of:
 - pupils
 - parents/carers
 - Staff

Scope of the Policy

This policy applies to all members of the school (including staff, students/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 eSafety 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 policy). In the case of both acts, action can only be taken over issues covered by the published 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 take place out of school.

Roles and Responsibilities

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

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 the deputy head teacher 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.
- The Headteacher, SLT and I.T Lead are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-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 e-safety monitoring role. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

E-Safety Coordinator (DSL):

- 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 eSafety incident taking place.
- provides training and advice for staff.
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports regularly to Senior Leadership.

Network Manager/Technical staff:

The Computing Lead is responsible for ensuring:

- that the school's technical infrastructure is secure as possible and is not open to misuse or malicious attack via the use of network vulnerability scans.
- that the school meets required e-safety technical requirements and any Local Authority / other relevant body 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.
- the filtering policy, 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 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 / website/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher /E-Safety Coordinator.



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 and understood e-Safety procedures and guidance within the Staff Code of Conduct.
- they report any suspected misuse or problem to the Headteacher for investigation.
- 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
- pupils understand and follow the e-safety and acceptable use policies.
- 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 Lead:

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.
- cyber-bullying.

Pupils:

- are responsible for using the school digital technology systems.
- 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 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 e-safety practice when using digital technologies out of school and realise that the school's E-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 school will take every opportunity to help parents understand these issues through parents' days, newsletters, letters, website and information about national/local eSafety campaigns/literature. 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.

Policy Statements

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 e.g. on social networking sites.
- 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. 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 students / 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, particularly in association with photographs.
- Images of pupils will be anonymised, with no facial features
- Pupils' work can only be published with the permission of the pupil and parents or carers.

Data Protection



Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 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.

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 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. Staff and pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g., by remote access).
- Users must immediately report, to the head teacher – 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) 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.
- 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 school website and only official email addresses should be used to identify members of staff.

Reviewed: October 2024