Booker Avenue Infant School

E-Safety Policy

2026-27

Context

We live in a digital age where technology is playing an ever-increasing part in our lives. It is changing the way we do things both inside and outside of school and although we recognise the benefits of technology, we must also be aware of the potential risks and ensure that all staff, governors, pupils and parents/carers associated with the school are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- access to illegal, harmful or inappropriate images or other content
- unauthorised access to/ loss of/ sharing of personal information
- the risk of being subject to grooming by those with whom they make contact on the internet
- the sharing/ distribution of personal images without an individual's consent or knowledge
- inappropriate communication/ contact with others, including strangers
- cyber-bullying
- access to unsuitable video/ internet games
- an inability to evaluate the quality, accuracy and relevance of information on the internet
- plagiarism and copyright infringement
- illegal downloading of music or video files
- the potential for excessive use which may impact on the social and emotional development and learning of the young person

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (eg Child Protection, Positive Behaviour and Anti-Bullying).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential through good educational provision to build pupil's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with the risks.

The school must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks.

Scope of the Policy

This policy applies to all members of the school community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out of 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 incident of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

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.

E-Safety Roles and Responsibilities

Governors

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors on the Curriculum Committee and the Safeguarding Governor receiving regular information about e-safety incidents and monitoring reports.

Headteacher and SLT:

- are responsible for ensuring the safety (including e-safety) of members of the school community
- responsible for ensuring that the Computing Co-ordinator and other relevant staff receive suitable CPD training to enable them to carry out their e-safety roles and to train other colleagues as relevant
- 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 also support to those colleagues who take on important monitoring roles
- will receive regular monitoring reports from the Computing Co-ordinators
- 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

Computing Co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking pace
- provide training and advice for staff
- liaise with ICT technical staff – MGL – which is provided under contract
- receive reports of e-safety incidents and create a log of incidents to inform future e- safety developments
- meet with the e-safety governor to discuss current issues and review incident logs
- attend relevant meetings

School Network Provider:

- responsible for ensuring that the school's ICT infrastructure is secure and not open to misuse or malicious attack as well as off-site access
- ensure that the school meets the e-safety technical requirements
- ensure that users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- 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

Teaching and Support Staff:

- ensure they have an up to date awareness of e-safety matters and of the current e-safety policy and procedures
- ensure they have read, understood and signed the school 'Staff Acceptable User Policy'
- report any suspected misuse or problem to the Computing Co-ordinator or Head for investigation

- only use official school systems for any digital communications with pupils and only on a professional level
- ensure that e-safety issues are embedded in all areas of the curriculum (Curriculum Leads responsible for this) and in other school activities
- ensure that pupils follow the school e-safety and acceptable use policy
- ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- monitor ICT activity in lessons, extracurricular and extended school activities
- ensure they are aware of e-safety issues related to the use of mobile phones, cameras and hand-held devices and that they monitor their use and implement current school policies with regard to these devices
- ensure 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 pace for dealing with any unsuitable material that is found in internet searches. This is highly unlikely due to the school's filtering policy but any breach should be reported immediately to the Head/SLT

Designated Safeguarding Leads

The DSL should be trained in e-safety issues and be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- cyber-bullying

Pupils:

- are responsible for using the school ICT systems in accordance with the 'Pupil Acceptable Use Policy', which they will be expected to sign before being given access to school systems
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access ti inappropriate materials and know how to do so
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking/use of images and 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 therefore take every available opportunity to help parents/carers understand these issues through newsletters and the website. Parents and carers:

- will be responsible for endorsing (by signature) the Pupil Acceptable Use Policy

Teaching and Learning

The internet is an essential element for education, business and social interaction. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils, and so the school has a duty to provide pupils with quality internet access as part of their learning experience:

- the school internet access will be designed expressly for pupil's use including appropriate content filtering
- pupils will follow the Kapow Computing scheme of work with content that is mapped to the Education for a Connected World Framework and the Teaching Online Safety in Schools DfE document
- pupils will be given clear objectives for internet use and taught what is acceptable and what is not
- pupils will be educated in the effective use of the internet to research. Including the skills of knowledge location, retrieval and evaluation
- when children are directed to websites as part of home learning they will have been checked for appropriateness by the teacher setting the learning

World Wide Web

The internet opens up new opportunities and is becoming an essential part of the everyday world for children: learning, homework, sharing are some of the legitimate and beneficial uses. However, there are inappropriate and undesirable elements that must be managed:

- if staff or pupils discover unsuitable sites, the URL, time and content shall be reported to the teacher who will then record the incident on the e-safety log which will be stored on the iPad trolley. The e-safety log will be reviewed termly by the Computing Co- ordinator.
- pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- the school will work with MGL to ensure filtering systems are as effective as possible

Social Networking

Social networking Internet sites provide facilities to chat and exchange information online. This online world is very different from the real one with the temptation to say and do things beyond usual face-to-face contact.

- Use of social networking sites in school is not allowed and will be blocked/filtered.
- All staff are advised not to have contact with parents and children on any social networking site.
- Pupils and parents will be advised that the use of social network spaces outside of school is inappropriate for primary aged children.
- Pupils will be advised never to give out personal details of any kind that may identify themselves, other pupils, their school or location.
- Pupils will be encouraged to only interact with known friends and family over the Internet and deny access to others, especially when gaming.
- Parents, pupils and staff will be advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber-bullying and defamatory comments.
- Any queries, refer to the social media policy.

Mobile Phones

Mobile phones present opportunities for unrestricted access to the internet.

- Pupils are not allowed to bring mobile phones to school.
- Staff should not use mobile phones to contact parents/carers. School staff must always use the school phone.
- Staff, including students and visitors, are not permitted to access or use their mobile phones within the classroom or on the playground.
- Staff may use their mobile phones for personal use in the staffroom during lunchtime or before/after school.
- Parents cannot use mobile phones on school trips to take phots of the children.

Digital/Video Cameras

Pictures, video and sound are not directly connected to the Internet but images are easily transferred.

- Pupils will not use digital cameras, iPads or video equipment at school unless specifically authorised by staff.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff 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 can be used but only if other devices are unavailable. These images must be deleted by the end of the day.
- Care should be taken when taking digital/video images that pupils are dressed appropriately and are not participating in activities that put them at risk or bring the individuals or the school into disrepute.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and comply with good practice guidance on the use of such images.
- Pupil's full names will not be used anywhere on a website, particularly in association with images.
- Permission from parents/carers will be obtained before photographs of pupils are published on the school website.
- The Headteacher will inform parents/carers and others present at school events that photographs/videos may be taken on the basis that they are for private retention and not for publication in any manner.
- Pupils must not take images or videos of others on iPads without their permission.

School Website

The school website is a valuable source of information for parents and potential parents.

- Contact details on the website will be the school address, email, telephone and fax numbers.
- Staff and pupil's personal information will not be published.
- The Head and SLT will take overall responsibility and ensure the content is accurate and appropriate.
- Photographs and videos that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupil's full names will not be used anywhere on the website, particularly in association with photographs
- Consent from parents/carers will be obtained before photographs of pupils are published on the school website.
- Parents/carers may upload pictures of their own children on to social networking sites. If the picture includes another child/children then it is their responsibility to gain permission from that child's parents/carers.
- The governing body may ban the use of photographic equipment by any parent who does not follow the school policy.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- E-safety will be discussed with MGL and those arrangements incorporated in our agreement with them.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate.

Prevent Statement

The Counter-Terrorism and Security Act 2015 places a statutory duty on named organisations, including schools, to have due regard towards the need to prevent people being drawn into terrorism. The most important part of this Act is 'keeping pupils safe from the danger of radicalisation and extremism'. Staff must know how to identify behaviour of concern and how to refer students who may be at risk of radicalisation for appropriate support. All Staff must update their Prevent Duty training on a regular basis.

The internet provides children with access to a wide range of content, some of which is harmful. Extremists use the internet, including social media, to share their message. The filtering systems we use at Booker Avenue Infant School block inappropriate content, including extremist content.

Where staff or pupils find unlocked extremist content they must report it to the Head or Computing Co-ordinator.

Cyber Bullying

- Pupils are taught to use the Internet safely and responsibly.
- Pupils learn what behaviour constitutes cyberbullying and its impact.
- Pupils learn how to handle concerns and report incidents.
- Pupils are encouraged to discuss any concerns or worries they have about online bullying and harassment with their teachers.
- Complaints of cyber bullying are dealt with in accordance with our Positive Behaviour and Anti-Bullying Policy.

Handling E-Safety Complaints

- Complaints of internal internet misuse will be dealt with by the Head.
- Any complaint about staff misuse must be referred to the Head.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents/carers will be informed of the complaints procedure.

Communication of Policy

To pupils:

- rules for internet use will be displayed in all networked rooms
- pupils will be informed that internet use will be monitored
- pupils will look at different areas of safety through the digital learning lessons

To Staff:

- all staff will be given the school e-safety policy and its importance explained
- staff should be aware that internet traffic can be monitored and traced to the individual user discretion and professional conduct is essential

To parents/carers:

- parents/carers attention will be drawn to the school e-safety policy on the school website
- they will receive regular updates on e-safety via leaflets and e-mail
- parents/carers will be encouraged to discuss code of conducts with their children before they are then asked to sign the 'Pupil Acceptable Use Policy'

Review

This policy will be reviewed annually