## Safety Policy

### Policy Statement

(INSERT SCHOOL NAME HERE) SCHOOLS recognizes the benefits and opportunities which new technologies offer to teaching and learning. We provide internet access to all learners and staff and encourage the use of technologies in order to enhance skills, promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards within the school while supporting staff and learners to identify and manage risks independently and with confidence. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies.

In furtherance of our duty to safeguard learners we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant school policies e.g. Safeguarding, Acceptable Use and applies to all members of the school community (including staff, students, volunteers, parents / guardians, visitors and community users) both in school and out of school. It is a statement of the aims, principles, strategies and procedures for e-safety throughout the school. The policy provides the framework to nurture a safe digital community.

### Definition of E-Safety

E-Safety refers to child protection and safeguarding of both children and adults in the digital world. It is about learning to understand and use technologies in a safe, positive way, also about supporting children and adults to develop safe online behaviors (both in and out of school).

**Risks to children who use the internet include:**

* Exposure to inappropriate materials, for example, pornographic pictures and videos
* Physical danger and sexual abuse, for example, through ‘grooming’ by pedophiles
* Cyberbullying – persistent bullying through the digital medium
* Losing control over pictures and videos
* Obsessive use of the internet and ICT, for example, addiction to video games
* Damage to online reputation
* Inappropriate or illegal behavior, for example, exposure to hate mail or offensive images
* Viruses, hacking and security
* Copyright infringement, for example, the illegal sharing of music, pictures, video or documents

**There are also risks to staff who use the internet.**

E-Safety is largely concerned with internet communications. The internet is accessible from computers, laptops, tablets, mobile phones, games consoles and other devices like the iPod Touch and internet connected TV. Other communication technologies such as texting and phone calls are also covered by the term ‘E-Safety’.

The technologies covered by this policy are computer, Internet, electronic communication and mobile devices such as mobile/smart phones and PDAs. Current Internet technologies used both inside and outside of the classroom include:

* + Websites
  + Virtual Learning Environments
  + E-mail and Instant Messaging
  + Chat Rooms and Social Networking
  + Blogs and Wikis
  + Podcasting
  + Video and Music Downloading

Students may be working online in school, at home or elsewhere. They may be using personal devices not covered by school security systems and everyone to needs to understand the risks and act accordingly.

### School Policy on the Use of the Internet

* Pupils will be taught what internet use is acceptable and what is not. They will be given clear objectives for internet use.
* Staff should guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
* Internet access will be planned to enrich and extend learning activities.
* Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.
* Pupils are required to return a signed copy of the Internet Acceptable Usage Agreement for Pupils every year which must be countersigned by their parent or guardian.
* All staff and visitors to school must read and sign the Internet Acceptable Usage Agreement for Staff and Community Users before using any school ICT resources.
* Pupils will be encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.
* Pupils will be taught to question information before accepting it as true.
* School internet access will be filtered appropriate to the ability of the pupils to use it within school rules.
* The school will ensure that use of internet derived materials by staff and pupils complies with copyright law

### School Policy on the Use of Email

* Staff and pupils may only use official school email accounts on school devices. Personal email accounts are not to be used.
* All emails sent must be professional in tone and content.
* Personal email accounts must not be used for communication between staff and students or parent/guardians.
* Personal information (as defined in the Personal Data and Information Sharing Policy) must not be emailed to external email addresses from school email accounts as emails are sent in an unencrypted format which is not secure.
* Personal information must not be emailed from staff to the official school email address and vice versa, as emails are sent in an unencrypted format which is not secure.
* Pupils must have adult supervision whilst using email.
* Pupils must immediately tell a teacher if they receive offensive email.
* Pupils must not reveal personal details of themselves or others in email communication (such as address or telephone number). Pupils must not arrange to meet anyone without specific permission.
* Email sent to an external organization should be written carefully and authorized by a member of staff before sending.
* Pupils will be made aware that the writer of an email (or the author of a web page) may not be the person claimed.

### School Policy on the Use of Social Networking Platforms

Social networking sites (like Facebook, Twitter or MySpace) are online ‘communities’ of internet users with similar interests. Members of the community create an online ‘profile’ which provides other users with varying amounts of personal information. Once users have joined the network, they can communicate with each other and share things like music, photos and films. The sites are a fun way to stay connected with friends, family and peers. However, as with most potential online dangers, the problems can start if you do not look after personal information properly.

**Workers at the school shall:**

* Behave responsibly and professionally at all times in connection with the use of social networking sites.
* Ensure that all communication with pupils (including on-line communication) takes place within clear and explicit professional boundaries.
* Raise any concerns to the Principal that any colleague(s) is/are not acting in accordance with this policy.
* Use their professional judgment and, where no specific guidance exists, take the most prudent action possible and consult with the Principal if they are unsure.
* Co-operate with management in ensuring the implementation of this policy.
* Respect the privacy and feelings of others.
* Keep a professional distance from pupils and ensure a clear separation of the private social lives of workers at the school and those of pupils.

**Students at the school shall:**

* NOT publish personal information like location, email address, phone number or date of birth.
* Be very careful about what images and messages are posted, even among trusted friends – once they are online they can be shared widely and are extremely difficult to get removed.
* Keep a record of anything abusive or offensive received and report any trouble to the site management (most sites have a simple reporting procedure, normally activated by clicking on a link on the page).
* Be aware that publishing or sharing anything which would mean breaking a copyright agreement is illegal.
* If you make an online friend and want to meet up with them in real life, ensure you have a responsible adult with you to check the person is who they say they are.
* Be aware of online scams – offers which seem too good to be true usually are.
* Do not to get into any online discussions about sex as this tends to attract potentially dangerous users.

### School Policy on the Use of Chatrooms and Instant Messaging

* The use of these facilities is not permitted in school.

### School Policy on the Use of Video Conferencing and other Video Communications

* Visitors/contributors may be invited to join (supervised) lessons through Skype or video conference in accordance with the Visitor to School Policy.
* Pupils will not be allowed unsupervised access to video communications.
* Digital communication may take place between staff and students or parents/guardians using only official monitored school systems and must be professional in tone and content. Official school systems include: school email, official emails/texts, school website, official school twitter accounts.

### School policy on the Use of Mobiles, Cameras and Portable Digital Devices

**Pupils:**

* Mobile phones, tablets, portable electronic games and media players brought into school by pupils must be handed-in at the school office unless the Principal has given permission eg for communication aids.
* If a pupil is found to be in possession of one of these electronic devices, the school has authorized staff to search for such devices (in accordance with school policies) where they reasonably suspect that the data or files on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules.
* The sending of abusive or inappropriate text messages is forbidden.

**Staff:**

* Use of personal devices in school such as computers, tablets and any other device with the functionality to take pictures, videos or make sound recordings, is not permitted. Exceptions to this rule are personal mobile phones and any device with specific written permission from the Principal.
* Staff may only use personal mobile phones in designated areas. These areas are the Admin Team offices, the staff room and the car park.
* Use of personal mobile phones in school must be within the Internet Acceptable Usage Agreement.
* Staff must not keep or use personal mobile phones in view of children (eg if there are pupils in the staff room or offices)
* Staff must not use personal devices to take any images, video or sound recordings of pupils.
* Staff must not use school devices to take inappropriate images of children or images of children in non-designated areas (non-designated areas include toilets and changing rooms).
* Staff are allowed to take digital photographs and video images to support educational aims, but follow guidance in the Internet Acceptable Usage Agreement for Staff and Community Users concerning the taking, sharing, distribution and publication of those images.
* Text messaging must not be used for communication between staff and pupils unless used for the educational benefit of pupils with all parties using school-issued devices and specific written permission has been obtained from the Principal.
* Staff who are issued with tablets must sign the appropriate agreement (see appendices)

### School Policy on the Use of Memory Sticks and Other Portable Storage

This includes portable USB flash drives and portable hard disk drives.

* Hefty fines may be imposed on schools and individuals who lose personal data or allow it to escape into the public domain. The loss of an unencrypted memory stick containing the names of pupils would count. The school has therefore taken the decision to ban the use of memory sticks and portable hard disk drives in school (other than those used for backup purposes by the Network Manager in accordance with school policies). There will be sanctions for any breach of this policy.
* Memory sticks or portable hard disk drives may be used in exceptional circumstances with specific written permission from the Principal.
* Media card readers may be used to retrieve photos and video from school-owned camera cards (eg SD cards)
* The school’s Data Protection and Information Sharing Policy applies.

### School Policy on the Use of Optical Discs

School data in any form (documents, pictures, videos etc) will not be burned to CD or DVD except:

* When archiving data to be stored securely at school
* When submitting pupil work to examining bodies
* With specific written permission from the Principal.

### School Policy on the Use of the School Website

* The point of contact on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published.
* Website photographs that include pupils will be selected carefully and will only be published with parental permission.
* Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
* The Principal will delegate editorial responsibility to the Network & Premises Manager to ensure that content is accurate and quality of presentation is maintained.

### School Policy on Cyberbullying

Cyberbullying is the use of the internet and related technologies to harm other people, in a deliberate, repeated, and hostile manner. When children are the target of bullying via mobile phones, gaming or the internet, they can often feel very alone and, a once previously safe and enjoyable environment or activity, can become threatening, harmful and a source of anxiety.

* Pupils will be taught about the effects of cyberbullying.
* Pupils will be encouraged to keep any evidence of cyberbullying.
* Pupils will be made aware that the police will be able to trace the originator of any messages.
* Cyberbullying (along with all forms of bullying) will not be tolerated in school. All incidents reported will be recorded and investigated.

### School Filtering Procedures

* The school Filtering Policy applies.
* The school will work in partnership with the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
* If staff or pupils discover an unsuitable site, the URL, content, user who made the discovery, time it was discovered and device that was being used must be reported to the Network Manager. If appropriate, the Network Manager will filter the site and/or inform the Internet Service Provider in order for the site to be filtered for all schools.

### School Monitoring Procedures

* Logs of internet activity will be regularly checked.
* Pupil and staff files stored on school computers will be regularly checked.
* Pupil and staff emails will be regularly checked.
* Pupil and staff use of social networking websites will be regularly checked.
* Illegal misuse will be dealt with in accordance with stipulated sanctions.

### School ICT and Data Security

* The school Data Protection and Information Sharing Policy applies
* The school Password Security, Filtering and the ICT Service Continuity Management requirements apply.
* Users must not share their user account details and must not leave their computers unlocked and accessible to others.
* Official remote communication channels into schools systems will be encrypted.
* Users of the official school remote access system must sign the (INSERT SCHOOL NAME HERE) SHOOLS Remote Access Agreement.
* Personal data sent over the internet will be encrypted.
* Unapproved system utilities and executable files are not permitted on school equipment.
* Remote access to school systems for email or Remote Desktop Services may be made from personally-owned computers, however, no files are to be saved to the computer and email attachments containing personal data should not be opened.
* No school data (pictures, videos, documents etc) other than that which is freely accessible on the school website, is to be stored on any computer other than those owned by the school.
* Loss of personal data must be immediately reported to the Principal, as an Information Risk Incident.
* Virus protection updates and system updates for PCs will be regularly installed.
* School ICT systems security will be reviewed regularly.

### Policy Enforcement

The E-Safety Co-ordinator will ensure that the E-Safety Policy is implemented and compliance with the policy monitored. Any unacceptable or illegal activities will result in disciplinary procedures being instigated.

**Pupils:**

* All pupils and their parents/guardians must sign the Internet Acceptable Usage Agreement for Pupils every year.
* The Internet Acceptable Usage Agreement for Pupils will often be referred to in lessons.
* E-Safety rules will be posted in all rooms where computers are used and will be discussed with pupils at the start of each academic year.
* Pupils will be informed that internet use will be monitored and sanctions will be imposed if the facility is abused.
* Any breaches of the Internet Acceptable Usage Agreement for Pupils will be referred directly to the E-Safety Coordinator.
* The school will keep a record of all pupils who have been denied internet access and the reason and length of time it was denied.
* Pupils will be informed that network and internet use will be monitored.
* Pupils' work will only be published with the permission of the pupil and parents.

**Staff:**

* All staff must read and sign the Internet Acceptable Usage Agreement for Staff and Community Users before using school ICT resources and annually thereafter.
* The school will keep a record of all staff who have been denied internet access and the reason and length of time it was denied.
* All staff including teachers, supply staff and support staff, will be told how to access this e-Safety Policy, and its importance will be explained.
* Staff will be made aware that professional conduct is essential when using school ICT and that internet use will be monitored and can be traced to the individual user.
* Any breaches of the Internet Acceptable Usage Agreement for Staff will be referred directly to the Principal.
* Implementation of the e-Safety rules will be checked regularly by the E-Safety Co-ordinator.
* The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective

### Handling Complaints

* Responsibility for handling incidents of internet misuse will be taken by the Family Support Advisor who will inform the E-Safety Coordinator.
* Any complaint about staff misuse of ICT must be referred to the Principal.
* Complaints of a child protection nature must be dealt with in accordance with school safeguarding procedures.
* Pupils and parents will be informed of the complaints procedure via the school website.
* Parents and pupils will need to work in partnership with staff to resolve issues.
* There may be occasions when discussions will be held with the Board of Directors to establish procedures for handling potentially illegal issues.
* Where possible the school will liaise with local organizations to establish a common approach to e-safety.

### Parental Support

* Parents' attention will be drawn to the school E-Safety Policy in newsletters, the school website, during e-safety events and during the annual e-safety week.
* Parents will be asked to read through the Internet Acceptable Usage Agreement for Pupils with their child and co-sign the agreement.
* Internet issues will be handled sensitively to inform parents without undue alarm.
* A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe internet use at home.

### Education & Training: Staff and Governors

There is a planned programme of e-safety training for all staff and governors to ensure they understand their responsibilities, as detailed in this, and the Internet Acceptable Usage Agreement for Staff and Community Users.

* All new staff receive e-safety training as part of their induction programme.
* The E-Safety Coordinator receives regular updates through attendance at training sessions and by reviewing regular e-safety updates from the local authority.
* This E-Safety Policy and its updates are shared and discussed in staff meetings. Updates are provided to all staff.
* The E-Safety Coordinator provides advice/guidance and training as required and seeks advice on issues where required.

### Education: Pupils

Whilst regulation and technical solutions are very important, their use must be balanced with educating learners to take a responsible approach. The education of students in e-safety is therefore an essential part of the school’s e-safety provision. Pupils need the help and support of the school to recognize and avoid e-safety risks and build their resilience.

* There is a planned e-safety scheme of work.
* Key e-safety messages are reinforced annually through an assembly and Safer Internet Week
* Pupils are helped to understand and act in accordance with the Internet Acceptable Usage Agreement for Pupils
* Pupils are taught to acknowledge the sources of information they use and to respect copyright when using material accessed on the internet.
* The Internet Acceptable Usage Agreement for Pupils is displayed in all rooms where ICT is used.
* E-safety is a focus in all relevant areas of the curriculum.
* In lessons where internet use is pre-planned, pupils are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches.
* Where pupils are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage pupils to use specific search terms to reduce the likelihood of coming across unsuitable material.
* Students are taught to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
* When using digital images, pupils are taught about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites
* Staff act as good role models in their own use of ICT
* Staff are familiar with and ensure that pupils act in accordance with the Internet Acceptable Usage Agreement for Pupils

### Development, monitoring and review of the policy

* This e-safety policy has been developed, and will be monitored, by our school e-Safety Committee which comprises:
  + Principal
  + E-Safety Coordinator
  + ICT & PSHE Subject Leader
  + Family Support Advisor
  + E-Safety Governor
  + Parent representative (TBA)
* Consultation with the whole school community has taken place through staff meetings, Student Council meetings, Governors meetings, E-Safety Week, the school website and the school newsletter.
* The school will monitor the impact of the policy using:
* Logs of reported incidents
* Logs of internet activity
* Other internal monitoring data
* Surveys of students, parents/guardians and staff (including non-teaching staff)
* Regular checks on school emails, users’ files, browsing history and staff and pupil use of social networking websites.
* The policy will be reviewed immediately where monitoring data shows a need. The policy will also be reviewed annually.