Howardian Primary School
E-Safety Policy - 2025

Introduction:

The 21st Century has witnessed an exponential increase in the number of children and young people who have embraced new technology as a mode of communication, socialisation, recreation and learning. Technology such as social media, email, mobile phones and games consoles are now a part of our society and a part of many of our daily lives. The benefits of such technologies are numerous and have changed and shaped the way in which we work, live and communicate with others. But as children of an increasingly younger age begin to use these technologies, there is a recognised need to educate and raise awareness with pupils of the risks, as well as the benefits, of new technologies.

E-Safety encompasses all Internet technologies and electronic communications such as mobile phones as well as collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.

Use of exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil achievement. The improper or unsafe use of technology can present challenges to children, young people, volunteers and staff.

There are a number of key risks to using new technologies, including:

- 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 exploitation and abused 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.
- Blackmail involving threats to life, dignity and violence.
- Poor or inappropriate supervision of Internet access leading to the viewing of harmful or inappropriate material.
- Risk of sexual exploitation.

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 (e.g. Positive Behaviour, Anti-bullying, Racial Equality and Safeguarding Policies).

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

At Howardian Primary School we strive to provide the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. The e-safety policy that follows explains how we intend to do this, while also addressing wider educational issues in order to help young people (and their parents / carers) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

This policy and any policies relating to the use of technology in school also applies when using technology for any form of distance learning for both staff and pupils.

Teaching and Learning:

At Howardian Primary School we have a duty to provide our pupils and staff with quality Internet access as part of their learning and teaching experiences. The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Access to the Internet is a necessary tool for staff and pupils. It helps to prepare pupils for their on-going learning and personal development needs. The purpose of Internet access in school is to raise educational standards, to support the professional work of staff and to enhance the school's management information and business administration systems.

Internet use enhances learning of pupils:

- **Internet access is provided by Cardiff Council and designed for pupils. This includes filtering appropriate to the content and age of pupils.**
- Internet access is planned to enrich and extend learning activities.
- Access levels are reviewed to reflect the curriculum requirement.
- Pupils are given clear objectives for Internet use and are only able to access the internet if permitted by a member of school staff
- Staff select sites which support the learning outcomes planned for pupils' age and maturity.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- Pupils are taught how to take responsibility for their own Internet access.
- Pupils are taught how to evaluate Internet content.
- Pupils are taught ways to validate information before accepting that it is necessarily accurate.
- Pupils are taught to acknowledge the source of information, when using Internet material for their own use.
- Pupils are made aware that the writer of an e-mail or the author of a web page might not be the person claimed.
- Pupils are encouraged to tell a teacher immediately if they encounter any material that makes them feel uncomfortable.

Managing Internet Access in School:

Internet access is provided by Cardiff Council via their school proxy servers and is designed for pupils. The follow systems are in place to ensure the safe provision of internet access:

- Cardiff Council provides their own firewall filtering.
- Our pupil iPads also have a profile which restricts access to age specific apps/videos/media content as well as a profanity and image filter.
- Children are not allowed to access videos on YouTube without the permission of an adult
- The school's ICT Leader conducts checks to ensure that the filtering methods selected are effective in practice.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the ICT Leader, who will report it to Cardiff IT to block.

Email

- Pupils are allowed to use school email accounts for school activities or when learning remotely (these are accessed through Hwb and they can only email other hwb addresses).
- Pupils must inform a teacher if they receive a rude, inappropriate or offensive email (pupils are taught to forward the email to the teacher and then delete it).
- In emails, pupils are taught that they must not reveal their personal details, those of others or arrange to meet anyone without specific permission.
- Pupils are taught not to open suspicious incoming emails or attachments.
- The forwarding of chain letters/emails is not permitted.
- Pupils will be taught that all emails are traceable and that once sent it will always be available.
- Parents are encouraged to monitor their child's email account on Hwb, including messages that they are sending.
- Pupils are only able to email other hwb addresses from their accounts.

Use of online learning platforms

At Howardian Primary School we use the Hwb platform for our online/remote learning in KS2 and Seesaw in the Foundation Phase, supported by activities from Active Learn. Other online apps may be used as deemed appropriate by school staff. The following is taught to our pupils and should apply if using these platforms in school or at home:

- Pupils should only login using their login details. if a device has been left logged in by someone else they are taught to log them out and sign in with their account.
- When working on a shared document, pupils should only work on their page. They can view other's work and read what they have done but they should not write anything on it unless given permission.
- Pupils will be taught that everything they write within Hwb is traceable (using 'previous versions' option) and that they should write appropriately at all times.
- Membership of shared drives (shared google drives and one drive) will be managed by the ICT Leader or class teacher. All teachers and pupils will have access while they are at the school. This list will be monitored with pupils and staff removed from the drives if they leave the school to ensure compliance with GDPR.

Photographing and publishing pupils' images and work

- Photographs must not identify individual pupils by their surname (first name and initial, if needed, are used, and only where necessary).
- Group shots or pictures taken 'over the shoulder' are used in preference to individual 'passport' style images.
- Children's photographs are only allowed to go online (website/ X / online publications etc) once permission has been received from the child's parent/carer.
- Children's work which goes online and contains a photograph of themselves must not contain the child's surname.

Social networking and personal publishing

See Social Media Policy for details of staff expectations and acceptable use. Pupils will not be allowed to access their own social media accounts or public chat rooms from a school device

Managing school resources / emerging technologies / video conferencing

- School devices are used by both staff and children for educational purposes.
- Staff iPads should not be used by pupils (with the exception of taking photos which does not give them access to all other apps) as they would have access to personal data.
- Mobile phones may be brought to school by year 5 & 6 pupils if they walk to or from school on their own. All pupil mobile phones must be turned off at the school gate and can only be turned on again once they leave the school premises. Children who bring mobile phones must hand them to their teacher at the beginning of the school day..
- *Video conferencing between staff should always use apps within Hwb (Teams or Meet) Other video conferencing facilities should not be used for school calls unless you are attending a course or meeting organised by an outside agency via a different platform (e.g. Zoom)*
- *Video conferencing with children should only be accessed by following advice from Cardiff IT/Welsh Government.*
- *Guidance is regularly being updated on this area so please seek up to date up to date advice from the ICT Leader if unsure. The following advice should be always be followed:*
    - *Only School devices should be used by staff when taking part in video conferencing with pupils*
    - *All parties involved should ideally be in a social space within their environment (ie downstairs - we recognise this will not always be possible for all pupils learning from home and teachers should use their professional judgement when assessing where children login from) Pupils sitting with wall behind them and/or use the blurred/virtual backgrounds greatly assists with this.*
    - *Teachers should record all live sessions and keep for future reference.*
    - *Teachers should consider their own environments when planning a call. Please ensure no personal information is viewable and that standards (what the children might hear or see) are the same as what you would expect in your classroom in school.*
    - *There should always be 2 members witnessing a call, either digitally (when children are working from home) or physically (in the same room as a call when working in school) or a combination of both.*
    - *On occasions, children may need to login to a lesson taking place in school from home (if they are self isolating etc) Different rules may be appropriate here for the number of adults on the call / camera on and off etc. Please seek the latest advice from the ICT Leader / Headteacher before using this method.*

- *Video calls, except for exceptional circumstances authorised by the Headteacher, should not take place on a 1:1 basis with a child.*

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the General Data Protection Regulation (2018) and be compliant with current GDPR practices.
- Staff must not keep confidential information (i.e. reports, class data etc) on removable devices such as USB devices unless it is the one provided by the school, which is encrypted.
- Staff can access Hwb through personal devices to view data or upload materials but they shouldn't download any data, photos or videos and store directly on these devices.
- Any personal device that saves their school / Hwb details must be password protected.
- There are very limited occasions where personal devices may need to be used for work purposes. These include:
  - Use of text /Whatsapp for school communication
  - Phoning parents when working from home / school
  - Uploading files to the staff drive, Hwb, SeeSaw or Google Classroom
  - Taking photos and uploading to school online media on a school trip, where this is the only means of internet connection (photos should be deleted from device once uploaded)
- *Reference – Personal Data & Passwords Policy*

Policy Decisions:

Authorising Internet access:

- All staff must read and sign the '**IT Acceptable Use Agreement for Staff and Volunteers**' before using any school resources.
- Parents/carers are asked to sign a consent form regarding their child's internet use (*see* **IT Acceptable Use Agreement for Pupils and Parents***).*
- Any person not directly employed by the school will be asked to read and sign the '**IT Acceptable Use Agreement for Staff and Volunteers**'' before being allowed to access computers or internet access from the school site.

Assessing risks

The school takes all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school, nor Cardiff Council can accept liability for any material accessed, or any consequences of Internet access. The school's e-safety policy and its implementation will be monitored and reviewed on a regular basis.

Handling e-safety complaints

- Complaints of internet misuse must be referred to the ICT Leader or Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher or Deputy Headteacher
- Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Policy.
- Pupils and parents are informed of the complaints procedure.
- Pupils and parents are informed of the consequences for pupil misuse of the Internet (see IT Acceptable Use for Pupils Agreement).

Communications:

Pupils and the E-Safety Policy

- Pupils take part in regular Internet safety days and information is sent home to parents.
- Pupils are informed that network and Internet use is monitored and appropriately followed up.
- The children receive e-safety lessons and are constantly reminded of online safety.

Staff and the E-Safety Policy

- ➢ All staff are updated regularly about e-safety and receive a copy of the e-safety policy.
- ➢ Staff are informed that network and Internet traffic can be traced to an individual user.
- ➢ Staff will show their class how a child friendly safe search engine can be used when accessing the internet with pupils. e.g. *Google Safe Search https://www.safesearchkids.com/*

Parents and the E-Safety Policy

- ➢ The school has links on its website to e-safety resources for discussion with children
- ➢ The school asks all new parents to sign the pupil/parent agreement when they register their child with the school.

The E-Safety Policy is reviewed regularly. - *However, due to the ever changing nature of digital technologies the policy can be reviewed and amended at any time in response to any significant new developments in the use of technologies, incidents or new threats to e-safety.*