High Down Schools

E-Safety Guidelines

Background / Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school.

The Internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and pupils learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe Internet access at all times.

These e-safety guidelines should help to ensure safe and appropriate use of the Internet and related communication technologies. The use of these technologies can put young people at risk within and outside the school, however through good educational provision, we aim to build pupils' resilience to, and understanding of, the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The following risks have been considered:

- 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 child/ young person.

Many of these risks reflect situations in the off-line world and the e-safety guidelines will be used in conjunction with the behaviour, anti-bullying and safeguarding policies. The e-safety guidelines that follow explain how we intend to help the children (and their parents) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.

Scope of the Guidelines

These guidelines apply to all members of the school community, including staff, pupils, volunteers, students, parents and carers, who have access to and are users of school ICT systems. They also apply to incidents of cyber-bullying, or other e-safety incidents within the terms of these guidelines, which may take place outside of the school, but are linked to membership of the school community.

The school will deal with such incidents within these guidelines 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 governors safeguarding working party reviews E-Safety as part of the overall safeguarding of children and reports to the Governing Body.

The ***Headteacher/ E-Safety Officer*** has a duty of care for ensuring the safety (including e-safety) of all members of the school community, though the day to day responsibility for e-safety will be delegated to the ***E-Safety Co-ordinator***.

The Headteacher:

- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- provides advice for staff and others and organises training as needed;
- liaises with external agencies, particularly in respect of child protection issues arising from e-safety work;

The E-Safety Co-ordinator:

- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety guidelines / documents;
- keeps up-to date with developments in relation to e-safety and disseminates these widely;
- helps ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- helps provide training and advice for staff and others;
- liaises with teaching and other staff in developing and evaluating e-safety educational programmes;
- liaises with the Local Authority / other relevant bodies;
- liaises with school technical staff.

Technical Staff are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack, including regular updating of virus protection;
- that the filtering system provided by SWGfL is applied effectively and consistently;
- that users may only access the networks and devices in line with the password guidelines;
- that user names/ access to school systems are updated e.g. when a member of staff leaves;
- that checks are carried out as required on staff laptops/ iPads;
- 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.

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current e-safety guidelines and practices;
- they read, understand and sign annually to state they will follow the Staff Acceptable Use Agreement (AUA);
- they report any suspected misuse or problem to the Headteacher/ E-Safety Coordinator / Officer;
- all digital communications with students / pupils / parents / carers are 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;
- personal data is handled securely (see e-mail and Data Protection sections below);
- pupils understand and follow the e-safety and acceptable use policies;
- pupils have an understanding of digital literacy and copyright issues appropriate to their age.

Pupils (as appropriate for their developing maturity)

- are responsible for using the school ICT systems in accordance with the Pupil Acceptable Use Guidelines which they will be expected to sign before being given access to school 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 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 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 Guidelines covers their actions out of school, if related to their membership of the school;
- have an age appropriate understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

Policy Statements

1. The importance of Internet use

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Because the Internet may be used within any curricular area and more widely within school, these E-Safety Guidelines should be adhered to at all times and within every aspect of school life.

2. Internet use enhances learning

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are required to return a signed copy of the ICT Acceptable Usage Agreement for Pupils every year, which must be countersigned by their parent or carer (in the case of Foundation Stage, parental signature only required).
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation, using a 'child-friendly' search engine. Google is not an appropriate search engine for children and the NEN gallery or Swiggle are used as alternatives.
- A planned e-safety curriculum is provided as part of Computing / PHSE / other lessons and is regularly revisited using a variety of approaches appropriate to the age and maturity of the children.
- Pupils are helped to understand the need for the pupil Acceptable Use Agreements and encouraged to adopt safe and responsible use both within and outside school
- Staff act as good role models in their use of digital technologies and the internet.

3. Pupils will be taught how to evaluate Internet content/ Digital Literacy

- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to question information before accepting it as true.
- Pupils are encouraged to tell a member of staff immediately if they find any material that makes them feel uncomfortable.
- From YR to Y2 pupils will take home an e-safety bag once a year, in addition to ongoing planned e-safety activities in school.

4. Educating parents and other carers

Many parents and carers may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, school web site
- High profile events / campaigns eg Safer Internet Day
- Reference to other relevant web sites / publications
- Other activities arising from parental suggestions or queries.

5. Education and training for staff

- A planned programme of formal e-safety training will be made available to staff. 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 guidelines and Acceptable Use Agreements.
- The E-Safety Coordinator / Officer (or other nominated person) will receive regular updates through attendance at external training events (eg from SWGfL / LA / other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- These E-Safety guidelines and updates will be presented to and discussed by staff in staff meetings / INSET days at least annually.
- The E-Safety Coordinator / Officer (or other nominated person) will provide advice / guidance / training to individuals as required.

6. Governor education and training

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / e-safety / health and safety / child protection. This may be offered in a number of ways e.g:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (eg SWGfL).
- Participation in school training / information sessions for staff or parents.
- Governor monitoring visits

7. E-mail

- Pupils must have adult supervision if using email.
- Staff and pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive or bullying email or any communication which makes them feel uncomfortable. They should not respond to such emails.
- Staff must immediately tell the Head teacher if they receive offensive or bullying email or any communication which makes them feel uncomfortable. They should not respond to such emails.
- Other members of the school community receiving offensive or bullying email or any communication which makes them feel uncomfortable should also be supported by the school.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation should be professional in tone and content, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Staff should only use school e-mail/ SchoolComms for communication with parents. Staff school e-mail accounts are subject to monitoring. If e-mails are redirected from a school e-mail to a personal (not shared) address they should be deleted once read. Replies must always be made from the school e-mail address.
- Personal information (as defined in the Personal Data and Information Sharing Guidelines – must not be emailed to external email addresses from school email accounts as it is not secure.
- Personal information must not be emailed from staff to the official school email address and vice versa, as it is not secure.

8. Published content and the school web site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- All images of children will have no names attached. All parents are required to sign annually to say that images of their children can be used.
- 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 eg on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is 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. 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.

9. Social networking and personal publishing/Cyber-bullying

- Staff follow the guidelines in the school social networking guidelines. All staff are expected to have read these guidelines and to abide by the guidance. Failure to abide by the guidance could result in disciplinary action.
- The school will block/filter access to social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils and parents will be advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- The E-Safety Co-ordinator will aid staff in passing on relevant information to share with parents regarding the age restrictions/recommendations provided from safe sources linking to social media sites/apps.
- School will continue to find suitable, up to date resources to show the dangers of the use of social media to any child in the school – and the reasons for age restrictions/recommendations through specified workshops/activities and lesson ideas from schemes of work.
- Any incidents of cyber-bullying will be reported directly to the Designated Safeguarding Lead. Any outside agencies such as police etc will then be notified and child protection procedures will be followed. Any pupil found to be involved with any misuse of the Internet at school or home (including cyberbullying) will have their access to the Internet taken away and this will be reviewed regularly. All incidents will be logged and regularly monitored, parents will also be informed.
- Other members of the school community affected by cyberbullying should also be supported by the school.

10. Managing filtering

- The school filtering system is provided by South West grid for learning (SWGfL).
- The school will work with the ICT support technician and the SWGfL to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover an unsuitable site, it must be reported to the Computing Subject Leader and E-Safety Co-ordinator.
- The Computing Subject Leader/ E-Safety Co-ordinator will ensure that regular checks are made so that the filtering methods selected are appropriate, effective and reasonable.

11. Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

We strongly discourage children bringing mobile phones to school. Staff mobile phones are not to be used in the classroom during contact time. Staff cameras and other mobile devices are not to be used during contact time. School mobiles are available for trips. Staff are permitted to take their own mobiles with them on trips in case of personal emergency but they are not to be used routinely. Parent helpers and others (students, volunteers) are required to sign a volunteer helpers' agreement covering the use of mobile devices and will be reminded about school guidelines on phones and cameras when on trips.

12. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. (Privacy Notice given to new parents)

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.
- Complete Freedom of Information requests within the required timeframe (see Freedom of Information Guidelines).

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.

13. Use of school ICT equipment away from school premises

The provisions of these guidelines apply equally to all school ICT equipment when used away from school premises.

14. Assessing risks

Access to the Internet will be by adult demonstration with directly supervised access to specific online resources.

The school will take all reasonable precautions to ensure that users access only appropriate 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 school computer. Neither the school nor Lighthouse Schools Partnership can accept liability for the material accessed, or any consequences of Internet access.

The school will audit ICT provision to establish if the e-safety guidelines are adequate and that their implementation is effective.

15. Complaints

- Responsibility for handling incidents of Internet misuse will be taken by the E-Safety Officer/ Co-ordinator.
- Any complaint about staff misuse of digital technology must be referred to the Head teacher.
- 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.
- There may be occasions when discussions will be held with the police support services to establish procedures for handling potentially illegal issues.
- Where possible the school will liaise with local organisations to establish a common approach to e-safety.

Communicating the E-Safety Guidelines

1. Introducing the e-safety guidelines to pupils
E-safety rules will be posted in all networked rooms and discussed with the pupils at the start of each year.
Pupils will be informed that network and Internet use will be monitored.

2. Staff and the E-Safety guidelines
All staff will be given the School E-Safety guidelines and Social Networking Guidelines and their importance explained.
Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct are essential.

If a colleague at the school believes they will have any difficulty complying with any of the requirements in these guidelines for whatever reason (for example, where they are related to a pupil), they should discuss the matter with the Headteacher/ the school designated safeguarding teacher/ officer. Failure to do so will be regarded as a serious matter.

3. Parental support
Parents' attention will be drawn to the School e-safety guidelines in newsletters, the school brochure, on the school web site and during the annual e-safety week.
Parents will be asked to read through the relevant ICT Acceptable Usage Agreement for Pupils with their child and co-sign it on an annual basis.

List of Relevant policies/guidelines

Password Guidelines
Staff Acceptable Use Agreement (AUA)
Pupils' Acceptable Use Agreements (AUAs)
Personal Data and Information Sharing Guidelines/ Privacy Notice
Photo permissions/ Internet usage sign up form
Social Networking Guidelines
Parent/ volunteer helpers agreement
Data Protection/ Freedom of Information Guidelines
Responding to incidents of misuse flowchart
Reporting log template