E - Safety Policy

This policy was adopted by the School Governing Body on

6th April 2022

Review Date: April 2023

This policy is part of the School's Statutory Safeguarding Approach. Any issues and concerns with e-safety must follow the school's safeguarding and child protection processes.

Contents

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

Appendices (download these documents as a zip file from osappendices.lgfl.net):

A1: Acceptable Use Agreement (Staff, Volunteers and Governors)

A2: Acceptable Use Agreements (Pupils – adapted for phase)

A3: Acceptable Use Agreement including photo/video permission (Parents)

A4: Protocol for responding to online safety incidents
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx - handling infringements
http://www.digitallyconfident.org/images/resources/first-line-information-support-HQ.pdf - page 23 onwards

A5: Prevent: Radicalisation and Extremism

A6: Data security: Use of IT systems and Data transfer

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation

1. Introduction and Overview

Rationale

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Hazeldown with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to deal with e-safety abuse such as online bullying.
- Ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our school community can be summarised as follows:

Content

- Exposure to inappropriate content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact

- Grooming (sexual exploitation, radicalisation etc.)
- Online bullying in all forms
- Social or commercial identity theft, including passwords

Conduct

- Aggressive behaviours (bullying)

- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and well-being (amount of time spent online, gambling, body image)
- Sexting
- Copyright (little care or consideration for intellectual property and ownership)

Scope

This policy applies to all members of the Hazeldown community (including staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of school IT systems, both in and out of Hazeldown.

Roles and responsibilities

Role	Key Responsibilities
Headteacher	• Will be adequately trained in off-line and online safeguarding, in-line with statutory guidance . • To lead a 'safeguarding' culture, ensuring that e-safety is fully integrated with whole school safeguarding. • To take overall responsibility for e-safety provision. • To take overall responsibility for data management and information security ensuring school's provision follows best practice in information handling. • To ensure the school uses appropriate IT systems and services including, filtered Internet Service, e.g. SWGfL services. • To be responsible for ensuring that all staff receive suitable training to carry out their safeguarding and e-safety roles. • To be aware of procedures to be followed in the event of a serious e-safety incident. • Ensure suitable 'risk assessments' are undertaken so the curriculum meets the needs of pupils, including risk of children being radicalised. • To receive regular monitoring reports from the Safeguarding Team. • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures. • To ensure Governors are regularly updated on the nature and effectiveness of the school's arrangements for e-safety. • To ensure the school website includes relevant information.

Role	Key Responsibilities
Safeguarding Team	• Take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the school's e-safety policy/documents. • Promote an awareness and commitment to e-safety throughout the school community. • Ensure that e-safety education is embedded within the curriculum. • Liaise with school technical staff where appropriate. • To communicate regularly with SLT and the designated safeguarding Governors to discuss current issues, review incident logs and filtering/change control logs. • To ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident. • To ensure that e-safety incidents are logged as a safeguarding incident. • Facilitate training and advice for all staff. • Oversee any pupil surveys / pupil feedback on e-safety issues. • Liaise with the Local Authority and relevant agencies. • Is regularly updated in e-safety issues and legislation, and be aware of the potential for serious child protection concerns.
Governors/Safeguarding Governors (including e-safety)	• To ensure that the school has in place policies and practices to keep the children and staff safe online. • To approve the E-Safety Policy and review the effectiveness of the policy. • To support the school in encouraging parents and the wider community to become engaged in e-safety activities. • The role of the Safeguarding Governors will include: regular review with the Safeguarding Team.
ICT Subject Leader	• To oversee the delivery of the e-safety element of the Computing curriculum.

Role	Key Responsibilities
IT Technician	• To report e-safety related issues that come to their attention, to the Safeguarding Team. • To manage the school's computer systems, ensuring - school password policy is strictly adhered to. - systems are in place for misuse detection and malicious attack (e.g. keeping virus protection up to date) - access controls/encryption exist to protect personal and sensitive information held on school-owned devices. • That they keep up to date with the school's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. • That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Safeguarding Team/Head teacher. • To ensure appropriate backup procedures and disaster recovery plans are in place. • To keep up-to-date documentation of the school's e-safety security and technical procedures.
Data and Information (Asset Owners) Managers (IAOs)	• To ensure that the data they manage is accurate and up-to-date. • Ensure best practice in information management. i.e. have appropriate access controls in place, that data is used, transferred and deleted in-line with data protection requirements. • The school must be registered with Information Commissioner.
Teachers	• To embed e-safety in the curriculum. • To supervise and guide pupils carefully when engaged in learning activities involving e-safety technology (including, extra-curricular and extended school activities if relevant). • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
All staff, volunteers and contractors.	• To read, understand, sign and adhere to the school staff Acceptable Use Agreement/Policy, and understand any updates. The AUP is signed by new staff on induction. • To report any suspected misuse or problem to the Safeguarding Team. • To maintain an awareness of current e-safety issues and guidance e.g. through CPD. • To model safe, responsible and professional behaviours in their own

Role	Key Responsibilities
	use of technology. **Exit strategy** • At the end of the period of employment/volunteering to return any equipment or devices loaned by the school. This will include leaving PIN numbers, IDs and passwords to allow devices to be reset, or meeting with line manager and technician on the last day to log in and allow a factory reset.
Pupils	• Read, understand, sign and adhere to the Student/Pupil Acceptable Use Agreement annually. • To understand the importance of reporting abuse, misuse or access to inappropriate materials. • To know what action to take if they or someone they know feels worried or vulnerable when using e-safety technology. • To understand the importance of adopting safe behaviours and 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. • To contribute to any 'pupil voice' / surveys that gathers information of their e-safety experiences.
Parents/carers	• To consult with the school if they have any concerns about their children's use of technology. • To support the school in promoting e-safety.
External groups including Parent groups	• Any external individual/organisation will sign on entry to the school to abide by the schools Acceptable Use agreement. • to support the school in promoting e-safety. • To model safe, responsible and positive behaviours in their own use of technology.

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website.
- Policy to be part of school induction pack for new staff.
- Regular updates and training on e-safety for all staff.
- Acceptable use agreements discussed with staff and pupils at the start of each year. Acceptable use agreements to be issued to whole school community, on entry to the school.

Handling Incidents:

- The school will take all reasonable precautions to ensure e-safety.
- Staff and pupils are given information about infringements in use and possible sanctions.
- Safeguarding Team acts as first point of contact for any incident.
- Any suspected online risk or infringement is reported to Safeguarding Team that day.
- Any concern about staff misuse is always referred directly to the Headteacher, unless the concern is about the Headteacher in which case the compliant is referred to the Chair of Governors and the LADO (Local Authority's Designated Officer).

Review and Monitoring

The e-safety policy will be reviewed when any significant changes occur with regard to the technologies in use within the school.

There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the school e-safety policy will be disseminated to all members of staff and pupils.

2. Education and Curriculum

Pupil e-safety curriculum

This school:

- Has a clear, progressive e-safety education programme as part of the Computing curriculum/PSHE and other curriculum areas as relevant. This covers a range of skills and behaviours appropriate to their age and experience;
- Plans e-safety use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas;
- Will remind students about their responsibilities through the pupil Acceptable Use Agreement(s);
- Ensures staff are aware of their responsibility to model safe and responsible behaviour in their own use of technology, e.g. use of passwords, logging-off, use of content, research skills, copyright;
- Ensures that staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright/intellectual property rights;
- Ensure pupils only use school-approved systems and publish within appropriately secure / age-appropriate environments.

Staff and governor training

This school:

- Makes regular training available to staff on e-safety issues and the school's e-safety education program;
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the E-Safety Policy and the school's Acceptable Use Agreements.

Parent awareness and training

This school:

- Provides information for new parents;
- Runs a rolling programme of e-safety advice, guidance and guidance via the school website and newsletters

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- Are responsible for using the school IT and communication systems in accordance with the relevant Acceptable Use Agreements;
- Understand the significance of misuse or access to inappropriate materials and are aware of the consequences;
- Understand it is essential to report abuse, misuse or access to inappropriate materials and know how to do so;
- Understand the importance of adopting good e-safety practice when using digital technologies in and out of school;
- Know and understand school policies on the use of mobile and hand held devices including cameras;

Staff, volunteers and contractors

- Know to be vigilant in the supervision of children at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Know to take professional, reasonable precautions when working with pupils, previewing websites before use; using age-appropriate (pupil friendly) search engines where more open Internet searching is required with younger pupils;

Parents/Carers

- Should provide consent for pupils to use the Internet, as well as other technologies.

Incident Management

In this school:

- There is strict monitoring and application of the e-safety safety policy and a differentiated and appropriate range of sanctions;

- All members of the school are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes;
- Support is actively sought from other agencies as needed (i.e. the local authority, SWGfL, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police) in dealing with e-safety issues;
- Monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the school;
- Parents/carers are specifically informed of e-safety incidents involving young people for whom they are responsible;
- The Police will be contacted if one of our staff or pupils receives communication that we consider is particularly disturbing or breaks the law;
- We will immediately refer any suspected illegal material to the appropriate authorities – Police, Internet Watch Foundation and inform the LA.

4. Managing IT and Communication System

Internet access, security (virus protection) and filtering

This school:

- Informs all users that Internet/email use is monitored;
- Has the educational filtered secure broadband connectivity through the SWGfL;
- Uses the SWGfL filtering system which blocks sites that fall into categories (e.g. adult content, race hate, gaming). All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Ensures network health through use of AVG anti-virus software;
- Uses encrypted devices or secure remote access where staff need to access 'protect-level' (sensitive personal) data off-site;
- Works in partnership with the SWGfL to ensure any concerns about the system are communicated so that systems remain robust and protect students.

Network management (user access, backup)

This school;

- Uses individual, audited log-ins for staff users;
- Ensures the Systems Administrator/network manager is up-to-date with SWGfL services and policies/requires the Technical Support Provider to be up-to-date with SWGfL services and policies;
- Has weekly back-up of school data (admin and curriculum).

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet, email access and network access. Online access to service is through a unique, audited username and password;
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins;
- Has set-up the network with a shared work area for staff. Staff are shown how to save work and access work from these areas;
- Requires all users to log off when they have finished working or are leaving the computer unattended;
- Ensures all equipment owned by the school and/or connected to the network has up to date virus protection;
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used primarily to support their professional responsibilities;
- Makes clear that staff accessing LA systems do so in accordance with any Corporate policies; e.g. email or Intranet; finance system, Personnel system etc;
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school/LA approved systems;
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need;
- Has a clear disaster recovery system in place that includes a secure, remote off site back up of data;
- This school uses secure data transfer; this includes DfE secure S2S website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted;
- Our wireless network has been secured to industry standard Enterprise security level /appropriate standards suitable for educational use;
- All IT and communications systems installed professionally and regularly reviewed to ensure they meet health and safety standards.

Passwords

This school

- makes it clear that staff and pupils must always keep their passwords private, must not share with others; If a password is compromised the school should be notified immediately;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password(s) private;

- We encourage staff to use STRONG passwords;
- We encourage staff to change their passwords regularly;
- We require staff using critical systems to use two factor authentication.

E-mail

This school

- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Will contact the Police if one of our staff or pupils receives an email that we consider is particularly disturbing or breaks the law.;
- Will ensure that email accounts are maintained and up to date;
- We use a number of SWGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product AVG, plus direct email filtering for viruses.

Pupils:

- Pupils are taught about the e-safety and 'netiquette' of using e-mail both in school and at home.

Staff:

- Staff can only use the LA or SWGfL email systems on the school system;
- Staff will use LA or SWGfL email systems for professional purposes;
- Access in school to external personal email accounts may be blocked.

School website

- The Head teacher supported by the Safeguarding team and the Governing body, takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- The school website complies with statutory DFE requirements;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- Photographs published on the web do not have full names attached. We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;

Social networking

Staff, Volunteers and Contractors

- Staff are instructed to always keep professional and private communication separate;
- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to pupils, parents/carers or school staff;
- School staff should not be online friends with any pupils/parents. Any exceptions must be approved by the Headteacher;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or local authority and personal opinions must not compromise the professional role of the staff member, nor bring the school into disrepute;
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Pupils:

- Are taught about social networking, acceptable behaviours and how to report misuse, intimidation or abuse through our e-safety curriculum work;
- Students are required to sign and follow our [age appropriate] pupil Acceptable Use Agreement.

Parents:

- Parents are reminded about social networking risks and protocols through additional communications materials when required;
- Are reminded that they need to ask permission before uploading photographs, videos or any other information about other people.

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings without appropriate permission;
- We have CCTV in the school as part of our site surveillance for staff and student safety. The use of CCTV is clearly signposted in the school. We will not reveal any recordings without appropriate permission.

5. Data security: Management Information System access and Data transfer

Strategic and operational practices

At this school:

- The Head teacher is the Senior Information Risk Officer;
- Staff are clear who are the key contact(s) for key school information (the Information Asset Owners) are;
- We ensure staff know who to report any incidents where data protection may have been compromised;
- All staff are DBS checked and records are held in a single central record

Technical Solutions

- Staff have secure area(s) on the network to store sensitive files;
- We require staff to log-out of systems when leaving their computer;
- All servers are in lockable locations and managed by DBS-checked staff;
- Details of all school-owned hardware will be recorded in a hardware inventory;
- Details of all school-owned software will be recorded in a software inventory;
- Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website;
- Where any protected or restricted data has been held we get a certificate of secure deletion for any server that once contained personal data.

6. Equipment and Digital Content

Mobile Devices (Mobile phones, tablets and other mobile devices)

- Please refer to the Policy for use of Mobile Phones.

Digital images and video

In this school:

- We gain parental/carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter/son joins the school;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- If specific pupil photos (not group photos) are used on the school website, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use;

- The school blocks/filters access to social networking sites unless there is a specific approved educational purpose;
- Pupils are taught about how images can be manipulated in their e-safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information;
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.