



Hopelands Preparatory School

38/40 Regent Street, Stonehouse, Gloucestershire, GL10 2AD

| | |
|---|---|
| Document Title | Online Safety policy 2024-2025 |
| Date Issued/Approved: | Prior to September 2022 |
| Date Valid From: | September 2024 |
| Date Valid To: | September 2025 |
| Author/Owner Responsible: | Maria Boix |
| This document replaces (exact title of previous version): | Online Safety policy 2023-2024 |
| Approval route: | Governors |
| Document Location: | Staff Portal>Policies>Child Protection>CP&SG Policies 2024-2025 |
| Related Policies: | Safeguarding Policy, KCSIE 2024, Acceptable Use, Taking storing and using images policy, Data Protection Policy |

INTRODUCTION

It is the duty of Hopelands School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;

- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use Policy, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Safeguarding
- Staff Behaviour;
- Health and Safety;
- Behaviour Management;
- Caring and Anti-Bullying;
- Acceptable Use Policy;
- General Communications (incl social media);
- Data Protection; and
- PSHE.

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Hopelands School, we understand the responsibility to educate our pupils on online-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online-safety and listening to their fears and anxieties as well as their thoughts and ideas.

SCOPE OF THIS POLICY

This policy applies to the school including the EYFS.

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, tablets, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

ROLES AND RESPONSIBILITIES

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The School's Safeguarding Governor is also the designated online-safety Governor.

2. The Head and the Senior Leadership Team

The Head is responsible for the safety of the members of the school community and this includes responsibility for online-safety on all school devices and the school's network. The Head has delegated day-to-day responsibility to the ICT/online-safety coordinator.

In particular, the role of the Head and the Senior Leadership team is to ensure that:

- a. all staff, in particular the ICT/online-safety coordinator are adequately trained about online-safety which includes understanding roles and responsibilities in relation to filtering and monitoring; and
- b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online-safety in connection to the school.

3. ICT/Online-safety coordinator

The School's ICT/online-safety coordinator is responsible to the Headteacher for the day-to-day issues relating to online-safety. The ICT/online-safety coordinator, has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current online-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

4. IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. This includes the school's filtering and monitoring systems (Sophos) on all school devices and networks. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the Head and ICT/online-safety coordinator.

5. Teaching and support staff

All staff are required to read and sign that they have understood the Acceptable Use Policy before accessing the school's systems. All staff receive safeguarding training which includes understanding roles and responsibilities in relation to appropriate filtering and monitoring systems and procedures.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online-safety issues which may arise in classrooms on a daily basis.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

7. Parents and carers

Hopelands School believes that it is essential for parents to be fully involved with promoting online-safety both in and outside of school. We regularly consult and discuss online-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Acceptable Use Policy.

EDUCATION AND TRAINING

1. Staff: awareness and training

New teaching staff receive information on Hopelands online-Safety (including roles and responsibilities in relation to filtering and monitoring) and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on online-safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online-safety, filtering and monitoring.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate online-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.

A record of concern must be completed by staff as soon as possible if any incident relating to online-safety occurs and be provided directly to the school's ICT/online-Safety Coordinator and Designated Safeguarding Lead.

2. Pupils: online-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for online-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote online-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about online-safety within a range of curriculum areas and Computing lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels Computing and usually via PSHE lessons, pupils are taught about their online-safety responsibilities and to look after their own online safety. Pupils can report concerns to the Designated Safeguarding Lead and/or the ICT/online-Safety Coordinator and any member of staff at the school.

From year one, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Caring and Anti-bullying Policy, which describes the preventative measures as well as the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead and or ICT/ e -Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3. Parents & Guardians

The school seeks to work closely with parents and guardians in promoting a culture of online-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

POLICY STATEMENTS

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for schoolwork. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff at Hopelands are permitted to bring in personal devices for their own use. They may use such devices in the main school staffroom or office and only during break-times and lunchtimes. Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

2. Use of internet and email

Staff

Staff must not access social networking sites, personal email or any website or personal email which is unconnected with schoolwork or business from school devices or whilst teaching / in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room or school office.

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the Head, Deputy Head, or ICT/online-Safety Coordinator the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Head, Deputy Head, Business Manager and/or ICT/ online-Safety Coordinator.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Hopelands School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
 - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
 - using social media to bully another individual; or
 - posting links to, or endorsing material which is discriminatory or offensive.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using any personal email address.

Pupils

The school expects pupils to think carefully before they post any information online, or repost, or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Head, Deputy Head or ICT/online-Safety Coordinator or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its wifi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils (and relevant staff) should contact Head or ICT/online-safety co-ordinator for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

Staff and pupils are expected to save all data relating to their work to their school laptop/ PC or to the school's central server or the school's encrypted memory sticks.

Staff devices should be encrypted if any data or passwords are stored on them. The school expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head, Deputy Head or ICT/online-Safety Coordinator.

4. Password security

Pupils and staff have individual school network logins and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

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 (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.) without the permission of the people identifiable in them (or the permission of their parents), nor should parents 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 this policy and the Acceptable Use Policy/Taking, Storing and Using Images Policy and the General Communications Policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.


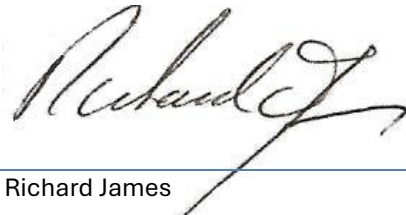
Pupils must not take, use, share, publish or distribute images of others. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images. Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

Hopelands will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy). The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Caring and Anti-Bullying Policy/Rewards and Sanctions Policy.

Complaints

As with all issues of safety at Hopelands, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online-safety prompt action will be taken to deal with it. Complaints should be addressed to the ICT/online-safety Co-ordinator in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate. Please see the Complaints Policy for further information. Incidents of or concerns around online-safety will be recorded using a Record of Concern form/ Incident Report form and reported to the school's Heads or ICT/online-Safety Co-ordinator and the Designated Safeguarding Lead, in accordance with the school's Safeguarding Policy.

| | |
|--|--|
| This policy was adopted at a meeting of | Hopelands Preparatory School |
| Held on | September 2024 |
| Date to be reviewed | September 2025 |
| Signed on behalf of the senior management team |  |
| Name of signatory | Maria Boix |
| Role of signatory | Headteacher |
| Signed on behalf of the Governing Body |  |
| Name of signatory | Richard James |
| Role of signatory | Chair of Governors |