



E-Safety Policy

The Safeguarding and Child Protection Committee is responsible for this policy.

Last Reviewed: January 2026

Introduction

It is the duty of Highfield Priory 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;
- AI based interactions and
- Mobile internet devices such as smart phones and tablets.

This policy, supported by the Acceptable Use policy for all staff, visitors and pupils, 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
- Health and Safety;
- Behaviour Management & Anti Bullying;
- Acceptable Use Policy;
- Data Protection;
- Bring Your Own Device (BYOD); and

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 Highfield Priory, we understand the responsibility to educate our pupils on e-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 e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

Scope of this Policy

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 (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, 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

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 Headteacher and the Senior Leadership Team

The Headteacher and DSL are responsible for the safety of the members of the school community and this includes responsibility for e-safety.

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

- a. staff, in particular the e-safety coordinator are adequately trained about e-safety; 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 e-safety in connection to the school.

E-safety coordinator/Head of CSIT

The School's e-safety coordinator is responsible to the Headteacher for the day to day issues relating to e-safety. The e-safety coordinator, has responsibility for ensuring this policy is upheld by all members of the school community, and works with all IT staff/SLT to achieve this. They will keep up to date on current e-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.

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. 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 e-safety coordinator and Headteacher.

Teaching and support staff

All staff are required to sign the Acceptable Use Policy before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

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.

Sanctions for pupils:

Sanctions will be applied dependent upon severity or the number of breaches. The following sanctions can be applied if a pupil commits a breach of the school's Acceptable Use Policy:

- A warning given by the e-Safety Coordinator to the pupil regarding the breach of the school's Acceptable Use Policy.
- After consultation with the Headteacher, letters to be sent home from the e-Safety Coordinator to parents/guardians detailing the misbehaviour.
- After consultation with the Headteacher, a meeting the parents/guardians and the e-Safety Coordinator to discuss the misbehaviour.
- After consultation with the Headteacher, a temporary or permanent ban for the pupil having Internet access.

Employees found to be in breach of the Code of Conduct for Staff will be disciplined in accordance with the arrangements specified in the Disciplinary Procedure.

Parents and carers

Highfield Priory believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. We use our social media channels to communicate important events/updates to parents using material and content from The National Online Safety Centre as a guide. 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

Staff: awareness and training

New teaching staff receive information on Highfield Priory's e-Safety and Acceptable Use policies as part of their induction.

All staff receive regular information and training on e-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 e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. 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 e-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 e-safety occurs and be provided directly to the school's e-Safety Coordinator and Safeguarding Lead.

Pupils: e-Safety in the curriculum

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

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

At age-appropriate levels, and usually via PSHE and Relationship Education and CSIT, pupils are taught about their e-safety responsibilities and to look after their own online safety. From year 5, pupils are both informally and formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Safeguarding Lead, the E-Safety Coordinator and any member of staff at the school.

From year 4, 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 Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the Safeguarding Lead and 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.

Tackling Extremism and Radicalisation

The procedures for dealing with instances of extremism and radicalisation are laid out within the applicable school policy. During the course of our studies it is possible that issues may be raised relating to aspects of fundamental British values and terrorism/radicalisation. We as a school are aware that these need to be handled with due consideration to our duties as stated under Prevent and the Channel Programme. All staff are aware of this and have taken part in radicalisation training. If any issue is raised in lessons which gives staff cause for concern they are aware of the process they need to follow and the appropriate member of staff they need to contact – the Safeguarding DSL - if they feel further guidance is required.

A significant element of our teaching and learning regarding Internet safety is applicable to this area. Tackling extremism and radicalisation is analogous to many of the issues covered by our duties under child safeguarding. Children are taught to be aware of potential dangers online and how to stay safe. The issue of anonymity is also covered so that children are made conscious of the fact that a stranger may be creating a false persona to entrap them. Extremist propaganda and radicalisation is directly discussed with Year 6 pupils during the unit about Internet safety and touch typing. In our Year 3 unit about searching computerised resources, explicit mention is made of the need to test the veracity of sources. The e-safety framework that is outlined in our e-Safety Policy is also directly applicable to dealing with threats of this nature and ensuring the safety of our pupils.

Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-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. The school recognises that not all parents and guardians may feel equipped to protect their children when they use electronic equipment at home. Regular advice and guidance is communicated through social media, parent emails and annual curriculum evenings.

Policy Statements

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. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the Staff and Visitors BYOD Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff at Highfield Priory are permitted to bring in personal devices for their own use. Staff are not allowed to use their personal devices during a lesson with children in the room. They may use such devices in the main school staffroom or when they are by themselves away from children. 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.

Pupils

No personal devices belonging to pupils are to be used during lessons at school, whether for schoolwork or personal use.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the pupil's class teacher and deputy headteacher to agree how the school can appropriately support the pupil.

Use of internet and email

Staff

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

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 e-Safety Coordinator / IT Technician 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 e-Safety Coordinator / IT Technician.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Highfield Priory 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 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. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils are issued with their own personal school email addresses for use by remote access through the virtual learning platform, Teams. Access is via a personal login, which is password protected.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to the e-Safety Coordinator / IT Technician / or another member of staff.

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 e-Safety Coordinator / IT Technician / or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file (CPOMS) and will be dealt with under the school's Behaviour Management Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact the IT Technician for assistance.

Data storage and processing

The school takes its compliance with GDPR 2018 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.

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 e-Safety Coordinator.

Highfield Priory fulfils the requirements of the General Data Protection Regulation (2018) with regards to how sensitive or personal data is recorded, processed, transferred and made available for access in school. We ensure that the data is:

- Accurate;
- Stored securely;
- Fairly, transparently and lawfully processed;
- Processed for limited, specified purposes;
- Processed in accordance with the data subject's rights;
- Adequate, relevant and not excessive;
- Kept no longer than is necessary;
- Only transferred to others with adequate protection.

Please refer to the guidelines and regulations stated in the General Data Protection Regulation Policy for further details. The school makes use of SharePoint for the storage of vital data. SharePoint allows us an additional degree of data security from viral/hacking attacks, as well as versioning and backup protection for documents, with the further benefit of being able to work on documents at home. Pastoral, assessment and organisational aspects of the school are stored within the Curriculum directory on SharePoint. The Curriculum folder has an immutable structure which staff have been informed that they must uphold.

Financial and organisational information is stored on SharePoint according to business function. We have directories for Building and Facilities Management, Governance, Human Resources, Policies and Procedures, and Business Shared. Every user has a personal area to store data on the network and the pupils have a shared drive called Work through which they can access files and documents provided to them by teachers.

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 term;
- not write passwords down; and
- not share passwords with other pupils or staff.

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 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 (see Parent Contract / Acceptable Use Policy for more information).

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.

Misuse

Highfield Priory 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 Anti-Bullying Policy.

Schedule for monitoring

The following monitoring schedule will apply to the e-safety policy:

The implementation of the e-safety policy will be monitored by:	CSIT Coordinator, Headteacher and IT Technician.
Monitoring will take place:	At regular intervals throughout the academic year and discussed at fortnightly IT meetings.
Should a serious online safety incident occur:	Headteacher, DSL, DPO and IT Technician.
Documents to be used when monitoring e-safety:	Acceptable Use Policy, Safeguarding Policy and Code of Conduct.

Complaints

As with all issues of safety at Highfield Priory, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Coordinator in the first instance, who will liaise with the leadership team and undertake an investigation where appropriate.

Authority

The Full Board of Governors, by delegation to sub-committees, is responsible for formulating the policies and procedures that will ensure the school continue to achieve the aims of the overall school strategy. Hence, each sub-committee has Terms of Reference and assigned responsibility for policies within that scope. The sub-committees are: Finance and General Purposes Committee, Health, Safety and Wellbeing Committee, Safeguarding Committee, Education Committee and Marketing Committee.