



e-Safety Policy

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

Last Reviewed: September 2026

Scope of this Policy

It is the duty of all staff at Highfield Priory School safeguard members of our community online, in line with statutory guidance and best practice. The school is aware of the wider statutory requirements that informs this policy.

This policy applies to all members of the school community who access or use school digital systems, including staff, learners, governors, volunteers, parents/carers, visitors and community users. It applies to use of school systems both on and off site, and to the use of personal devices on the school site (where permitted).

Where online safety concerns or incidents occur outside school and are known to the school, Highfield Priory School will respond in line with this policy and related procedures, including the school's Safeguarding, Behaviour and Anti-Bullying policies. Where appropriate, parents/carers will be informed of incidents involving inappropriate online behaviour that take place out of school.

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);
- PSHE and Citizenship Policy
- Relationship Sex and Health Education Policy

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 SLT will review this policy at least annually, or sooner in response to significant technological developments, emerging risks, or incidents.

Online safety is a shared responsibility. All members of the school community are expected to model safe, responsible behaviour, report concerns promptly and learn from incidents and good practice. The roles below clarify accountability.

Senior leaders set the culture and ensure that systems are effective. In line with [KCSIE](#), the DSL OSL (online safety lead) hold day-to-day lead responsibility. Senior leaders will:

- Ensure the school meets its safeguarding duty of care, including online safety.
- Know and apply procedures for serious allegations involving staff (Headteacher and DSL)
- Ensure that the DSL, OSL and relevant colleagues are trained and able to fulfil their roles.
- Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (both staff and pupil accounts)
- Ensure that children are taught about how to keep themselves and others safe online, through PSHE, RSE and Computing programmes, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.
- Put in place appropriate oversight and support for internal monitoring activity.
- Act on emerging risks and themes.
- DSL, OSL and Business Manager review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

Computing Lead/Online Safety Lead (OSL)

The OSL will:

- Lead the SLT and support the DSL day to day.
- Lead development and review of online safety and computing policies and curriculum
- Coordinate awareness, staff confidence and reporting readiness through appropriate training
- Map, embed and evaluate online safety education through Computing curriculum
- Work with PSHE and RSE coordinator to embed online safety education
- Keep up to date with risks across content, contact, conduct and commerce.
- Ensure key issues updated in KCSIE are addressed within the curriculum each year and explicitly taught, such as Generative AI and deepfakes being taught

Teaching and Support Staff

All staff are expected to uphold professional standards online and contribute to a strong safeguarding culture. Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate
- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.
- Ensure they are keeping up-to-date with OSL's direction when KCSIE updates are added to the curriculum so full coverage is taught to all pupils

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.

Pupils

Pupils will:

- Follow their Acceptable Use Policy agreements.
- Report concerns and know how to get help.
- Use technology responsibly, respecting others and their copyright and intellectual property.
- Will only access AI in a controlled manner through Purple Mash in school
- Understand that out-of-school behaviour may be addressed where it affects the school community.

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.

Other Users

Community users accessing school systems or platforms will sign an Acceptable Use agreement before access is provided. The school welcomes partnership working and shares good practice where appropriate.

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.

Online Safety Education at Highfield

Online safety education is a core part of the school's safeguarding approach and sits alongside effective technical controls (including filtering and monitoring). In line with KCSIE, online safety is a running and interrelated theme reflected across relevant policies and the curriculum.

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks (including [DfE "Teaching Online Safety in Schools"](#), [UKCIS "Education for a Connected World"](#)). Resources such as Purple Mash and 2BeSafe enable full coverage of Computing and online safety, whilst embedding cross-curricular skills from the PSHE and RSE curriculum.

<https://highfieldpriory.sharepoint.com/sites/Public/Shared%20Documents/Curriculum/Subjects/Computing/Online%20Safety%20Obj%20Whole%20School.xlsx?d=w280efc4f519c44ac8279f33f3c5b1688>

Learning is age-appropriate, builds on prior learning, is matched to need, and is taught through existing curriculum areas (including RSHE/RSE, Health Education, Computing and Citizenship), with teacher assessment and clear intended outcomes.

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries (including awareness of the [Computer Misuse Act 1990](#));
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing

- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing
- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

Where internet use is planned, learners are guided to appropriate resources, such as through Purple Mash in Computing lessons, and pupils will be supported if unsuitable content is encountered. Where open searching is permitted, staff supervise and remain vigilant. Filtering may be temporarily adjusted for legitimate curriculum research, with auditable approval and clear rationale.

Learner voice is actively used to strengthen the school's approach through feedback. Highfield Priory School has a Student Council for pupil voice and also uses pupil surveys for feedback. Learners are given appropriate opportunities to discuss changes affecting their digital lives and to express concerns about friendship, belonging, access, exclusion and wellbeing.

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. 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 DSL - if they feel further guidance is required.

A significant element of our teaching and learning regarding online 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. For example, in KS2 pupils learn how the internet can draw us to information of different agendas, what is meant by 'stereotypes' and how they can be reinforced online, and how people may present 'opinions' as 'facts'.

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, parents evenings and 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. School mobile phones have a red cover so that they are easily recognisable.

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 when children are present. They may use such devices in the main school staffroom or when children are not in the classroom for a designated period of time.

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. School does not permit mobile phone, smart watch use (of smart features) or meta glasses.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities, special educational needs or pupils who are young carers. 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. The pupil will be escorted to the office and supervised by staff accordingly in such situations.

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 it. They can find the DSL, Headteacher, Business Manager, Computing Lead or IT support staff. This will then be shared amongst necessary parties. 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 DSL, Headteacher and IT support staff.

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

There is strong anti-virus and firewall protection on our network. Filtering and monitoring is in place with Smoothwall.

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. They can find the DSL, Headteacher, Business Manager, Computing Lead or IT support staff. This will then be shared amongst necessary parties.

The school expects pupils to think carefully before they post any information online, 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 nearest member of staff, usually class teacher, who can then share with DSL, Headteacher, Business Manager and Computing Lead. 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.

Password security

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

All 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.

Pupils log ins are known to teachers to support logging in and remembering this information. Teachers are not to access pupil accounts without the pupils present. Purple Mash allows teachers to read and assess the curriculum work their pupils have created in the 'Work' section of their teacher accounts.

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. Highfield Priory School urges parents to consider their use of mobile phones, smart watches and meta glasses when on the school premises.

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). Purple Mash and 2BeSafe ensure the coverage of such information.

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. The Headteacher will remind parents of this at the beginning of each school show and production.

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 (part of National Crime Agency).

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the schools search policy outlined in the Behaviour policy and following Safeguarding policy protocol.

In line with KCSIE updated guidance, cyber security will be treated as outlined in the safeguarding policy. The DSL will be notified immediately and supported to deal with all instances by the SLT, DDSL's and Lancashire County Council, where appropriate.

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 and Behaviour Policies.

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 GDPR lead.

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.

EYFS

Our EYFS policy supports this online safety policy. Below is a brief summary of key information but more detailed information can be found p13 and 14 of the EYFS policy.

To ensure the safety and well-being of children we do not allow staff to use personal mobile phones or other personal devices with imaging and sharing capabilities during working hours.

We use mobile phones supplied by the School only to provide a means of contact in certain circumstances, such as outings or forest school.

Parents and carers are asked to refrain from using devices with imaging and sharing capabilities when in the setting.

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:	OSL, DSL, Headteacher
Monitoring will take place:	At least annually, but sooner if national updates occur e.g KCSIE
Filtering and monitoring meetings will take place regularly to discuss incidents and review practice (both staff and pupil accounts)	DSL and Business Manager
Should a serious online safety incident occur:	Headteacher, DSL, DPO and OSL
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 DSL and OSL 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: Audit and Compliance Committee, Education Committee, Finance and General Purposes Committee, Health, Safety and Wellbeing Committee, Safeguarding and Child Protection Committee and Sales and Marketing Committee.