HEREWARD HOUSE SCHOOL

Online Safety Policy

Author: Paul Cheetham (DSL)

Policy ratified by: SLT

Date of publication: 1st September 2026

Date of next review: August 2027

Governor responsible for policy: Governing Body

Hereward House School: Online Safety Policy

Our School's Aims

At Hereward House we aim to provide a warm, welcoming and safe atmosphere in which every child can thrive and feel comfortable. Whilst embracing the highest academic aspirations for our pupils, we strive to create a stimulating, purposeful and happy community, where every child feels valued and secure. Promoting the well-being of all pupils is at the heart of what we aim to do. For us the most important outcome is for all pupils to be kind, considerate and confident whilst looking out for every member of the school community. We aim to be a school where pupils will be encouraged and assisted to develop academically, morally, emotionally and culturally. It is our belief each pupil should enjoy their school days and reflect upon them with pride, pleasure and affection. We are preparing pupils not just for senior school, but for life.

Introduction

Hereward House School is committed to ensuring a warm, welcoming and safe atmosphere in which every child can thrive and feel comfortable. It is the school's duty to ensure 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 and abuse.

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 including: **websites, search engines, messaging services, social media, gaming platforms, livestreaming, artificial intelligence tools, mobile devices and emerging digital technologies**.

This 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.

- This policy should be read in conjunction with:

  - **Safeguarding and Child Protection Policy**
  - **Behaviour, Rewards and Consequences Policy;**
  - **Anti-Bullying Policy;**
  - **PSHE & RSHE Policies**
  - **Acceptable Use of AI Policy**
  - **Staff Code of Conduct**
  - **SEND Policy**

- **Complaints Policy**
- **Curriculum Policy (due to online safety through PSHE & ICT)**

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

At Hereward House, 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.

This policy covers both fixed and mobile Internet devices provided by the school (such as PCs, laptops, tablets, interactive whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought on to school premises (personal laptops, tablets, smart phones, etc.).

Roles and responsibilities

The Designated Safeguarding Lead (DSL), assisted by the ICT Lead, has responsibility for ensuring this policy is upheld by all members of the school community. They will keep up to date on current online safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

The Headteacher, alongside the IT Coordinator will:

. Ensure the policy is implemented, communicated and compliance with the policy is monitored

. Ensure staff training in online safety is provided and updated annually as part of safeguarding training

. Ensure immediate action is always taken if any risks or dangers are identified i.e. reporting of inappropriate websites (this will be picked up by our device management: Senso Monitoring which is externally monitored)

. Ensure that all reported incidents of cyber bullying are investigated

. Ensure appropriate web filtering software is used to protect users from potentially damaging/offensive material (Lightspeed web filtering)

Teachers and Staff will:

. Keep passwords private and only use their own login details, which are stored securely.
. Monitor and supervise pupils' internet usage and use of other IT resources
. Adhere to the Acceptable Use Agreement
. Promote online safety within school
. Engage in online safety training
. Only download attachments/material onto the school system if they are from a trusted source
. When capturing images, videos or sound clips of children, only use school cameras or recording devices

The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of staff members and the reputation of the school and the County Council are safeguarded. In this context, staff members must be conscious at all times of the need to keep their personal and professional lives separate.

The School recognises that pupils with Special Educational Needs and Disabilities (SEND) may be especially vulnerable to risks online. Staff are expected to consider pupils' individual needs when teaching online safety, applying the behaviour policy, or responding to incidents. The DSL and SENDCo will work together to ensure adjustments to filtering, access, or supervision are made where necessary, and individual risk assessments will be considered for pupils with more complex profiles.

- Please see **Staff Code of Conduct** or **School Safeguarding Policy** for further guidance.

Governors will:

. Ensure that the school is implementing this policy effectively.
. Adhere to the acceptable use agreement when in school.
. Have due regard for the importance of online safety in school.

Monitoring, Filtering and Oversight

Hereward House School: Online Safety Policy

The School recognises its statutory duty under KCSiE 2026 and the *DfE Filtering and Monitoring Standards (2023)* to ensure robust systems are in place for detecting and responding to harmful online behaviour. As part of our whole-school safeguarding culture, the following measures are in place to monitor and filter internet use and ensure a safe digital environment for pupils and staff.

1. Filtering and Monitoring Systems

- The School uses **Lightspeed web filtering**, which automatically restricts access to websites identified as inappropriate, including those promoting extremism, pornography, self-harm, or other harmful content.
- From **2026-27**, the School also operates **Senso Monitor**, a fully externally managed real-time monitoring system that flags high-risk behaviour — including signs of self-harm, suicide ideation, online grooming, stress, aggression, or bullying — across websites, offline documents, and search engines.
- All pupil internet access takes place via **school-owned and managed devices**, under direct supervision of staff, and within a secure network.
- Access to unregulated platforms and social media is disabled by default.

2. Roles and Responsibilities

- The **DSL** holds overarching responsibility for the strategic oversight of filtering and monitoring systems and ensures these are appropriate to the School's risk profile.
- The **IT Manager** manages technical configuration and updates to filtering lists, working in partnership with Senso's external monitoring team and Lightspeed's reporting tools.
- Weekly or incident-based reports are reviewed by the **DSL/SLT**, and safeguarding referrals are made where required, in line with the School's Safeguarding and Child Protection Policy.
- The **Headmaster and Governors** ensure that filtering and monitoring systems are reviewed regularly for effectiveness and are proportionate to the needs of pupils of different ages.

3. Review and Risk Assessment

- The School will **review the effectiveness of its filtering and monitoring provision at least annually**, and:
    - After any significant safeguarding incident involving online safety;

  - When new technologies or platforms are introduced;
  - When updates to DfE/KCSiE guidance are issued.
- The DSL and IT Manager conduct a **risk assessment** of the digital environment, considering the needs of vulnerable pupils (including those with SEND), and the specific risks associated with Reception to Year 8 settings.

4. Incident Response and Escalation

- Any pupil or staff member who encounters harmful or inappropriate content must report it **immediately** to a member of staff or directly to the ICT Lead and DSL.
- Inappropriate sites encountered by pupils will be recorded, investigated, and blocked as appropriate.
- Any activity flagged by Senso or Lightspeed as high-risk will be reviewed by the DSL, logged on CPOMS, and responded to in accordance with safeguarding procedures.
- **All filtering or monitoring alerts** that involve safeguarding risk will be handled in line with the School's **Safeguarding and Child Protection Policy** and may involve liaison with external agencies or parents.

Working in Partnership with Parents

The school believes that it is essential for parents/carers to be fully involved with promoting online safety both in and outside school. We regularly consult and discuss online safety with parents/carers and seek to promote a wide understanding of the benefits and risks related to Internet usage. It is the responsibility of the ICT Lead to deliver online safety advice talks to parents, educating parents on current online dangers, personal data safety tips, popular website and social media uses with each year group and tips for setting online security settings.

Staff awareness

New teaching staff receive information on personal online safety and acceptable Internet use on school premises, 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 pupils within the context of online safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. When

pupils use school computers, staff should make sure they 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.

If any incident relating to online safety occurs it must be reported to the Deputy Head and IT Co-Ordinator as soon as possible. If a staff member is concerned that the incident may be a safeguarding concern it must be reported directly to the school's DSL in line with the school's Safeguarding and Child Protection Policy.

The ICT Lead coordinates the online safety curriculum, working closely with PSHE leads to ensure that online safety themes are explicitly taught and age-appropriate across all year groups. This includes the delivery of core content through ICT lessons, PSHE sessions, and assemblies. The curriculum mapping is reviewed annually and overseen by SLT. All staff are expected to reinforce key messages across subjects and settings as part of the school's broader safeguarding culture. Staff are also required to complete the Educare Module – online safety so that they are provided with up to date knowledge and skills and are able to teach good practice.

Consequently, staff should be able to understand the unique risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online at school. If any member of staff feels they need further training in this area they are encouraged to speak to the Deputy Head about this. We wish to create an environment where staff have a clear voice on training in this area.

KCSIE 2026 contains a wealth of resources and information for staff.

Online and school community

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 builds resilience in its pupils by providing them with opportunities to learn about online safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE, as well as informally, when opportunities arise.

At age-appropriate levels, and usually via PSHE and ICT lessons, pupils are taught to look after their own online safety. Using CEOP material, pupils are informally taught about recognising and reporting aspects of cyber bullying and online sexual exploitation, stalking and grooming.

Pupils are taught about the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL, their form teacher and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the Internet; such as data protection, intellectual property and legal age limits on certain Social Media websites and mobile apps. As part of the School's pupil 'Acceptable Internet Use Agreement' (please see Appendix 1), pupils are taught about respecting other people's information and images (etc.) through discussion and classroom activities.

It is the responsibility of the ICT Lead to provide tailored online safety advice talks to Forms 3-CE1, giving advice on safe searching online, appropriate website use, personal data safety tips and possible implications of inappropriate use of pupil photographs, the Internet, social media, or mobile communication technologies.

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).

We also recognise that a one size fits all approach may not be appropriate for all children, and a more personalised or contextualised approach for more vulnerable children, victims of abuse and some SEND children might be needed.

Management of online safety incidents

. There is strict monitoring and application of the online 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. MASH, UK Safer Internet Centre helpline, CEOP, Prevent Officer, Police, IWF) in dealing with online safety issues.
. Any attempts to access inappropriate internet content on school, or personal technologies are automatically blocked and recorded by the school's secure content filtering and monitoring system. Details of such incidents are accessible by the ICT Lead and must be reported to the DSL and the Head teacher. Relevant sanctions will then be taken.
. Monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school.
. Parents/carers are specifically informed of online safety incidents involving young people for whom they are responsible.
. The Police will be contacted if one of our staff or pupils receives online 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 MASH.

Use of school and personal technology devices

Staff

School Devices

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 school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Staff are not permitted to access inappropriate Internet sites on school, or personal technology devices, either in class or out of class. (The school's secure Internet content filtering system ensures this is possible). Any inappropriate access tried to gain will be recorded and reported to the ICT coordinator by the school's content filtering software. This will then be reported directly to the school's DSL immediately and formal disciplinary actions will be imposed.

Personal mobile phones and mobile devices

Staff are permitted to bring in personal devices for school related work use, however, no personal data should be projected onto interactive whiteboards in classrooms for pupils to see. A full virus scan must also be run on any personal technology, prior to connecting to the school server, every time it is used. It is the responsibility of the ICT Lead (where possible) to ensure this is done. In the event that the ICT Lead is unavailable, it is the responsibility of the Deputy Head to ensure this is done. If personal technology devices are used on School premises by staff, or visitors, no content or images related to pupils, should be stored on these personal technology devices at any time.

Staff may use their mobile telephone on school premises, but must do so out of sight of pupils, in the staff common room. Staff members are not allowed to use personal technology devices within the EYFS setting under any circumstances. All such equipment must be turned off and out of sight at all times in an EYFS setting.

Personal telephone numbers should not be shared with parents/carers and under no circumstances may staff contact a pupil using a personal telephone number.

Visitors

Any visitors to the School may use a School or personal computer for school related work, while on School premises, though no access to the school server is to be granted and all internet access can only be accessed via the school's secure Wi-Fi connection, which implements our internet content filtering system, to ensure no inappropriate content is accessed. Again, it is the responsibility of the ICT Lead to ensure this is done, through a secure Wi-Fi policy connection.

Pupils

No personal devices belonging to pupils are to be used during lessons at school. Permission may be been granted by the Headmaster for a pupil to use a personal laptop for typing in class. In such a scenario, all pupil devices must have a thorough virus scan run by the ICT Lead before allowing the device to be connected to the secure school network. All personal devices used by pupils for typing in lessons will be set up by the ICT Lead to 'onboard' to the school's private and secure pupil Wi-Fi connection, which will grant access to the pupil drive on the school server and wirelessly access a school printer. This connection disables all internet access and only grants access to the pupil area of the school network, for saving and accessing pupil lesson files. All other internet and Wi-Fi access will be blocked. All pupils using personal devices (and their parents) must agree to these terms of use.

Any technology device used by pupils in school (school, or personal) will be granted limited access to the school network for security reasons. School devices used by pupils will be accessible via pupil logins, only allowing pupils to access the pupil network drive and the Internet, through a content filtering system, or have internet access blocked through different pupil security logins.

Any attempt to access inappropriate content on a school, or personal technology device on school property will be automatically recorded, blocked and will be emailed to the ICT coordinator and reported directly to the DSL and the Headmaster.

If pupils bring in mobile phones (e.g. for safety purposes if they walk to and from school alone), they should be kept switched off and left with the school office at the beginning of the school day. They may then be collected at the end of the school day.

Use of Internet and email

All teaching and support staff are provided with a school email address. Staff should use this address when sending work-related emails. Staff should be aware that all emails can be retrieved at a later date should this be necessary. Staff emails should never be used to forward 'chain' or 'junk' email. Staff should not communicate with pupils via email

Staff

Staff must not access social networking sites and any website or personal email which is unconnected with school work or business from school devices or whilst teaching or in front of pupils. Such access may only be made whilst out of sight of pupils.

When accessed from personal 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.

There is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications are monitored. All Internet use is filtered through an Internet content filtering system, which runs on all school computer devices connecting to the internet through the school's wired or Wi-Fi connections. This restricts any access to websites deemed to contain inappropriate material and any attempt to access such websites Is recorded under the user's login profile.

Staff must immediately report to the Headmaster 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.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Hereward House 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 or material which is discriminatory, offensive, or inappropriate to pupils.

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

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 a 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

Acceptable Internet Use Policy

It is the responsibility of SMT and all teaching staff to ensure all pupils who access the Internet on school premises adhere to the pupil Acceptable Internet Use Policy, which outlines rules to adhere to when accessing the Internet and named websites/types of software pupils agree not to access on school premises.

There is strong anti-virus, firewall protection and secure content filtering on our network. Spam Emails, certain attachments and websites will be blocked automatically by the system.

If this causes problems for school work/research purposes, pupils should contact the ICT Lead for assistance.

Pupils should immediately report, to the Deputy Head or ICT Lead 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.

Pupils must report any accidental access to materials of an inappropriate nature directly to the Deputy Head, ICT Lead or another member of staff. Deliberate access to any will be dealt with under the school's Behaviour, Rewards and Consequences Policy. Pupils should be aware that all attempted Internet usage via the school's systems and its Wi-Fi network is monitored, whether via school, or personal computer.

Pupil's Online Safety – At School

In line with the school's aim to provide a welcoming and safe atmosphere, in which every child can thrive and feel comfortable, the school takes online safeguarding extremely seriously. As part of the school's online safeguarding strategy, the school has a stringent Internet content filtering system in place, which restricts any access to websites deemed to contain inappropriate material. This filtering system is imposed on all school technology accessing the Internet via the school's network. Pupils using the school's secure WiFi connection on their personal devices will automatically have the internet blocked on their machine while connected to our network.

It is the responsibility of the DSL to ensure this content filtering system is set up on all school technology accessing the Internet. It is also the responsibility of the DSL to regularly check (and when necessary, update) the list of 'blocked sites', to ensure continued pupil online protection.

Pupil's Online Safety - At Home

Helpful online safety advice is given to all pupils from F3-CE1 each term, through eSafety ICT lessons, school assemblies and pupil online safety advice talks (mentioned in the Online safety in the curriculum and school community section of this policy).

Several sites offer helpful advice to parents, particularly with respect to how they can best monitor their child's use of the computer at home. Important and useful information can be found on the following site:

Career and Education Resources - National Cybersecurity Alliance

EYFS Pupils

Screen Time and Use in the EYFS

The School recognises that both the amount of time children spend using screens and the way in which screens are used are important in the Early Years.

Screen time in the EYFS is limited and will not normally exceed one hour during the school day. Staff will aim to keep screen use below this level wherever possible and will be mindful that children may also spend time using screens at home.

Where screens are used, this should be planned and purposeful, with a clear educational benefit. Staff should engage with children during screen use rather than allowing prolonged solitary or passive viewing. Content must be checked in advance and should be age-appropriate and suitable for young children. Content containing advertising, scrolling feeds or autoplay features should not be used.

Screen use should support, rather than replace, high-quality interaction between children and adults, physical activity, creative and imaginative play and opportunities for children to explore their environment. Screens should not be used simply to occupy children, manage behaviour or as a routine means of calming a child. Screens should also be avoided during mealtimes.

These limits do not apply to assistive technology used to support a child with SEND where its use provides a clear communication, wellbeing or quality-of-life benefit. Such use will be considered according to the individual needs of the child.

Digital devices may be used by staff to support assessment and record observations, but their use should be proportionate.

AI tools, including toys or devices with built-in AI features, will not ordinarily be used directly with EYFS children unless the School is satisfied that their use is appropriate and supports children's development.

For the purposes of this policy, screen use includes tablets, laptops and desktop computers, mobile phones, televisions, gaming devices, interactive whiteboards and touchscreens, e-readers, smart watches, video platforms and screen-enabled toys.

Prevent Awareness

Staff need to be aware of any pupils who may be in contact with or being targeted by violent extremists. Pupils are particularly at risk through the use of internet and social media, either at home or at school. Both the DSL and Governor with responsibility for safeguarding have undertaken Prevent awareness training. The school has a robust filtering system that ensures that pupils are safe from terrorist or extremist material when accessing the internet through the school system.

If there is evidence that a pupil is becoming deeply enmeshed in the extremist narrative, schools should seek advice from Camden's Integrated Youth Support Services on accessing programmes to prevent radicalisation under the Channel project.

Although decisions to seek support for a child in need, or about whom there are concerns relating to radicalisation, would normally be taken into consultation with parents and pupils, their consent is not required for a referral when there are reasonable grounds to believe that a child is at risk of significant harm.

Further advice for staff and governors can be sought from the DfE dedicated helpline and mailbox: 020 7340 7264 and counter-extremism@education.gsi.gov.uk

Data storage

The school takes its compliance with the UK GDPR and the Data Protection Act 2018 seriously. Staff and pupils are expected to save all data relating to their work to the school's central server, where data backups are automatically made on a nightly basis.

Staff devices should be encrypted if any data or passwords are stored on them. The school does not expect removable media to be 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.

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

Password security

Staff have individual school network logins, emails and storage folders on the server. Staff 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 6 months;
- not write passwords down; and
- should not share passwords with 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).

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the UK GDPR and the Data Protection Act 2018). To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites (etc.), nor should parents/carers comment on any activities involving other pupils in the digital/video images.

Staff and volunteers are allowed to take digital/video images using school devices, (camera or iPAD) to support educational aims, but must follow this policy and the Safeguarding and Child Protection 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 without their permission.

Written permission from parents or carers will be obtained before photographs of students/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 if used in association with photographs.

Cyber-Bullying

Central to the School's anti-bullying procedure is the stance that bullying is not tolerated in any form. This includes through electronic communication either inside or outside of school. Under powers granted by the EIA 2006, Hereward House School is able to police cyber-bullying or any bullying aspects carried out by pupils even at home.

Definition of Cyber-Bullying

Cyber-bullying is an aggressive, intentional act carried out by a group or individual using electronic forms of contact repeatedly over time against a victim who cannot easily defend himself/herself.

By cyber-bullying, we mean bullying by electronic media:

- Bullying by texts or messages or calls on mobile phones
- The use of mobile phone cameras to cause distress, fear or humiliation
- Posting threatening, abusive, defamatory or humiliating material on websites, to include blogs, personal websites, social networking sites
- Using e-mail to message others
- Hijacking/cloning e-mail accounts
- Making threatening, abusive, defamatory or humiliating remarks in chat rooms, or on Social Media websites to include Facebook, Instagram, Youtube and Ratemyteacher

Legal Issues

There is not a specific law which makes cyberbullying illegal but it can be considered a criminal offence under several different acts including Protection from Harassment Act (1997), Malicious Communications Act (1988), Communications Act (2003) Obscene Publications Act (1959) and Computer Misuse Act (1990).

Policy & Staff Training

Hereward House School educates its pupils both in the proper use of telecommunications and about the serious consequences of cyber-bullying and will, through PSHE and in ICT lessons and assemblies, continue to inform and educate its pupils in these fast changing areas.

The school trains its staff to respond effectively to reports of cyber-bullying or harassment. This training is regularly updated: staff should receive safeguarding and child protection updates (including online safety) at Inset at the beginning of each term, to provide them with the skills and knowledge to safeguard children effectively. Staff are also required to complete the Educare Module – online safety so that they are provided with up to date knowledge and skills and are able to teach good practice.

The school endeavours to block access to inappropriate web sites, using firewalls, antivirus protection and secure content filtering systems and no pupil is allowed to work on the Internet without a member of staff present. Where appropriate and responsible, the school audits ICT communications and regularly reviews the security arrangements in place.

Whilst education and guidance remain at the heart of what we do, the school reserves the right to take action against those who take part in cyber-bullying.

All bullying is damaging but cyber-bullying and harassment can be invasive of privacy at all times. These acts may also be criminal acts.

- The school supports victims and, when necessary, will work with the Police and CEOP (Child Exploitation and Online Protection) to detect those involved in criminal acts.
- The school will use, as appropriate, the full range of sanctions to correct, punish or remove pupils who bully fellow pupils or harass staff in this way, both in and out of school.
- The school will use its power of confiscation where necessary to prevent pupils from committing crimes or misusing equipment.
- All members of the School community are aware they have a duty to bring to the attention of the Headmaster any example of cyber-bullying or harassment that they know about or suspect.

Guidance for Staff

If you suspect or are told about a cyber-bullying incident, follow the protocol outlined below:

Mobile Phones

- Ask the pupil to show you the mobile phone.
- Note clearly everything on the screen relating to an inappropriate text message, image, or social media post, to include the date, time and names.
- Take a screen shot photograph of the inappropriate material displayed on screen.
- Make a transcript of a spoken message, again record date, times and names.
- Tell the pupil to save the message/image.
- Go with the pupil and see the Headmaster, Deputy Head or in their absence, a member of the SMT.

Computers

- Ask the pupil to get up on-screen the material in question.
- Ask the pupil to save the material.
- Print off the offending material straight away.
- Make sure you have got all pages in the right order and that there are no omissions.
- Accompany the pupil, taking the offending material with you, to see the Headmaster or Deputy Head.
- Normal procedures for interviewing pupils and taking statements will then be followed particularly if a safeguarding issue is presented.

Guidance for Parents

It is vital that parents and the school work together to ensure that all pupils are aware of the serious consequences of getting involved in anything that might be seen to be cyber-bullying. The school informs parents of the cyber-bullying policy and the procedures in place to deal with cyber-bullying. The school also provides yearly safety talks for parents in Forms 3-CE1, outlining the school's policies on pupil's Internet use and providing safety tips to keep their son safe online.

- Parents can help by making sure their child understands the school's policy and, above all, how seriously the school takes incidents of cyber-bullying.
- Parents are given the option of signing a 'Parent/Child Agreement' which they can read through together, deciding on their own terms and conditions for online use at home and at school. (See Appendix 2)
- Parents should also explain to their sons legal issues relating to cyber-bullying.
- If parents believe their child is the victim of cyber-bullying, they should save the offending material (if need be by saving an offensive text on their or their child's mobile phone) and make sure they have all relevant information before deleting anything.
- Parents should contact the Headmaster as soon as possible. A meeting can then be arranged with the Headmaster, which may involve other relevant members of staff
- If the incident falls during the holidays, the school reserves the right to take action against bullying, perpetrated outside the school, which spills over into the school.
- Parents are encouraged to report/encourage their son to report any inappropriate content found, or inappropriate website behaviour to CEOP, using their 'report' button on the website: https://www.ceop.police.uk/Ceop-Report/.

Guidance for Pupils

In addition to regular eSafety ICT lessons, the school also provides regular safety assemblies/ talks to educate its pupils on legal issues of Internet usage, the dangers of using certain websites/social media and tips for personal data protection and safe use of the Internet.

- If you believe you or someone else is the victim of cyber-bullying, you must speak to an adult as soon as possible. This person could be a parent/guardian, your tutor, or the Headmaster.
- Do not answer abusive messages but log and report them.
- Do not delete anything until it has been shown to your Form Teacher, parents/guardian or the Headmaster (even if it is upsetting, the material is important evidence which may need to be used later as proof of cyber-bullying.)
- Do not give out personal IT details.
- Never reply to abusive e-mails.
- Never reply to someone you do not know.
- Always stay in public areas in chat rooms.

Complaints

As with all issues of safety at Hereward House School, 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 Headmaster (DSL) in the first instance, who will undertake an immediate investigation and liaise with the leadership team and any members of staff or pupils involved. Please see the Complaints Policy for further information.

Online safety and cyber bullying issues relating to safeguarding and child protection will be addressed by the Headmaster in his role as DSL, acting in accordance with the school's Safeguarding and Child Protection Policy.

National Bodies

Further support and guidance may be obtained from the following:

CEOP

Childnet

UK Safer Internet Centre

NSPCC

Internet Matters

DfE Filtering Standards

Monitoring & Review of this Policy

This policy will be reviewed annually by the DSL, ICT Lead, and SLT. The review will include analysis of incident logs, feedback from staff, pupils, and parents, and updates to statutory guidance. A report summarising findings will be shared with Governors and inform staff training and curriculum planning.

Appendix 1

Acceptable Internet Use Agreement

The school maintains computers and Internet access to help our learning. The rules you agree to follow in this agreement will keep everyone safe and help us to be fair to others.

- I will ask permission from a member of staff before using the Internet;
- I will not access another person's files without that person's permission;
- I will use the computers only for school work and homework;
- I will only e-mail people I know, or who my teacher has approved;
- The messages I send will be polite and sensible;
- I will not take, use or publish pictures of other people without their permission;
- I will not give my home address or phone number, or arrange to meet someone, unless my parent or teacher has given permission;
- To help protect other pupils and myself, I will tell a teacher if I see anything I am unhappy with or I receive messages I do not like;
- I understand that the school may check my computer files and may monitor the Internet sites I visit;
- I will not bring the school into disrepute when using social media and the Internet off site. I will be careful to avoid any behaviour that might be construed as bullying, including the deliberate exclusion of boys from online group conversations.

Appendix 2

Parent / Child Agreement

It is my goal to use the Internet in a manner that is safe and responsible. I know that my online actions reflect the kind of person I am. The following are my personal standards for online activities.

I will protect my personal privacy by:

I will protect my personal reputation by:

I will treat others online in the following way:

The kind of sites and activities I will avoid include:

If I am communicating with someone I do not know in person, the steps I will take to make sure this person is safe are:

If I become worried that someone I am communicating with online is not safe (to me or to other children), I will:

The following are the steps I will take to keep myself safe if I ever want to meet an online stranger in person:

If I receive a communication from someone that is inappropriate or upsetting, I will:

If someone treats me badly online, including sending repeated inappropriate messages, or posting material elsewhere that damages my reputation or friendships, I will:

The amount of time that I will spend online during a typical day is:

The strategies I will use to ensure my online activities do not interfere with homework and other important tasks are:

If I see material posted online that makes me worried that someone else might be in danger, or might cause harm to others, I will:

I will ask you for assistance if:

Other commitments I make are:

Appendix 3: Summary of Changes to the Online safety and Cyber Bullying Policy (2026–27)

The following updates and amendments have been made as part of the 2026–27 policy review:

1. Policy Structure and Content

- Combined all relevant updates into a cohesive and streamlined structure, improving readability and clarity.
- Reordered and clarified sections under: Roles and Responsibilities, Monitoring, Filtering & Safe Use, Curriculum and Staff Awareness.

2. Systems and Oversight

- Added details of new externally monitored safeguarding and filtering systems in place for 2026–27:
    - **Senso Monitor** for real-time alerts on self-harm, bullying, grooming, and online risk.
    - Use of **Lightspeed** for web filtering and alerts.

3. Roles and Responsibilities

- Clarified role of DSL, Deputy Head, ICT Lead, and teaching staff in monitoring, responding to and teaching online safety.
- Highlighted Governor oversight responsibilities for implementation.

4. Staff Training and Awareness

- Emphasised that online safety is included in **new staff induction** and ongoing **INSET training**.
- Staff now complete the **Educare Online Safety module**.
- Added encouragement for staff to **raise training needs** to Deputy Head.
- Explicit link to **Annex B of KCSiE 2026** to support professional knowledge.

5. SEND and Vulnerable Pupils

- New section added to reflect the need for **reasonable adjustments** and **differentiated support** for pupils with SEND in relation to online safety and cyber bullying (in line with KCSiE 2026 and Equality Act 2010).

6. Staff and Pupil Voice

- Confirmed staff are encouraged to feed back on online safety provision and request further training.

- Agreed to develop **pupil voice mechanisms** to inform future review and planning of online safety education and pastoral response.

7. Policy Links and Cross-References

- Strengthened policy signposting, including direct links or references to:
    - Safeguarding & Child Protection Policy
    - Behaviour, Rewards and Consequences Policy
    - Anti-Bullying Policy
    - SEND Policy
    - PSHE & RSHE Policy
    - Staff Code of Conduct
    - Acceptable Use of AI Policy

8. Strategic Planning and Monitoring

- Clarified that online safety curriculum is mapped across ICT and PSHE and reviewed annually.
- Added processes for **incident tracking** through CPOMS and DSL logging.