Howden Junior School

e-Safety Policy

Safeguarding Pupils,

Staff and Schools in a Digital World

September 2024

Please Note: This policy is to be followed in conjunction with the GDPR guidelines.

Table of Contents:

1. Acknowledgements

This document is based on an original document '**School/Academy Online Safety Policy Template'** produced by the SWGfl E-safety Officer and adapted by Howden Junior School, September 2020. The policy was updated in September 2024 in line with the KCSIE 2024 (DFE) document.

At Howden Junior School we have the following policies in place that should be read in conjunction with this policy:

- Child Protection Policy
- Anti-bullying Policy
- Behaviour Policy
- Remote Learning Policy
- SEND Policy
- PSHE Policy
- RSHE Policy
- Child on Child Abuse Document
- GDPR
- Social Media Policy

2. Policy Introduction

This e-Safety policy recognises our commitment to e-safety and acknowledges its part in the school's overall Safeguarding policies and procedures. It shows our commitment to meeting the requirements to keep pupils safe in the 'Every Child Matters' agenda.

We believe the whole school community can benefit from the opportunities provided by the internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the steps we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. Our expectations for responsible and appropriate conduct are formalised in our Acceptable Use Policies (AUP) which we expect all staff and pupils to follow.

As part of our commitment to e-Safety we also recognise our obligation to implement a range of security measures to protect the school network and facilities from attack, compromise and inappropriate use and to protect school data and other information assets.

The aims of our policy are;

- To set out the key principles expected of all members of the school community at Howden Junior School with respect to the use of IT-based technologies.
- To safeguard and protect the children and staff of Howden Junior School.
- To assist school staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with pupils.

3. Scope of the Policy

- This policy applies to the whole school community including Howden Junior School's Senior Leadership Team, school board of governors, all staff employed directly or indirectly by the school, all pupils, parents and volunteers who have access to the school's digital technology system, both in and out of school.
- Howden Junior School's Senior Leadership Team and school board of governors will ensure that any relevant or new legislation that may impact upon the provision for e-Safeguarding within school will be reflected within this policy.
- The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyberbullying, or other e-Safeguarding-related incidents covered by this policy, which may take place out of school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.
- The school will clearly detail its management of incidents within this policy, associated behaviour and anti-bullying policies and will, where known, inform parents and carers of incidents of inappropriate e-Safeguarding behaviour that takes place out of school.

4. Review and Ownership

- The school has appointed an e-Safeguarding coordinator who will be responsible for document ownership, review and updates.
- The e-Safeguarding policy which has been written jointly by the school e-Safeguarding Coordinator, Mr Gary Johnson and the Chair of Governors, Mrs Julie Palmer. It is current and appropriate for its intended audience and purpose.

- The school e-Safeguarding policy has been agreed by the Senior Leadership Team and approved by governors.
- The e-Safeguarding policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The School has appointed a member of the governing body to take lead responsibility for e-Safeguarding. This will be Mrs Julie Palmer, current Chair of Governors.
- All amendments to the school e-Safeguarding policy will be shared in detail with all members of teaching staff.

Schedule for Development and Monitoring:

This online safety policy was approved by the Board of Directors/Governing Body/Governors Sub Committee on:	*September 2024*
The implementation of this online safety policy will be monitored by the:	*E-Safety Coordinator and Senior Leadership Team*
Monitoring will take place at regular intervals:	*Annually*
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	*September 2025*
Should serious online safety incidents take place, the following external persons/agencies should be informed:	*LA Safeguarding Officer, DSL, LADO, Police*

The school will monitor the impact of the policy using:

- Logs of reported incidents, via Cpoms.
- Monitoring logs of internet activity including sites visited/filtering (see more in section 8).
- Surveys/questionnaires of pupils, parents/carers and staff annually.

5. Communication of the Policy

- The Howden Junior School's Senior Leadership Team will be responsible for ensuring all members of staff and pupils are aware of the existence and contents of the school e-Safeguarding policy and the use of any new technology within school.
- The e-Safeguarding policy will be provided to and discussed with all members of staff annually.
- All amendments to the policy will be published and sessions to inform school members of the relevant updates to be held for all members of the school community when required.
- Any amendments will be discussed by the School Council[1] to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An e-Safeguarding or e-Safety unit will be included in the computing curricula covering and detailing amendments to the e-Safeguarding policy. This will be done at the start of the new school year in each year group.
- When required, e-Safety updates or e-safeguarding training is to be provided at staff meetings.

- E-Safeguarding or e-Safety training will be part of the transition programme across the Key Stages and when moving between establishments, pupils' responsibilities regarding the school e-Safeguarding policy will be reviewed.
- Pertinent points from the school e-Safeguarding policy will be reinforced across the curriculum and across all subject areas when using IT equipment within school.
- The key messages contained within the e-Safeguarding policy will be reflected and consistent within all acceptable use policies in place within school.
- We endeavour to embed e-Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The e-Safeguarding policy will be introduced to the pupils at the start of each school year, using the AUP, which will give the children the key points using child-friendly language that they can understand.
- E-Safeguarding posters will be prominently displayed around the school and in each classroom.

6. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school.

6.1: Responsibilities of the Senior Leadership Team

- The headteacher is ultimately responsible for all Safeguarding provision (including e-Safeguarding) for all members of the school community, though the day-to-day responsibility for e-Safeguarding will be delegated to the e-Safeguarding coordinator.
- The Headteacher and (at least) another member of the Senior Leadership Team will be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regards to e-Safety effectively.
- Support the e-Safety coordinator in their work.
- Receive and regularly review e-Safety incident logs and be aware of the procedure to be followed should an e-Safety incident occur in school.
- Develop and promote an e-Safety culture within the school community.
- When in the process of employing new staff within the school, SLT should carry out online searches of the candidates shortlisted for a position. This should be done to identify any incidents or issues that have happened, which are available online, which the school may wish to explore with applicants during the interview process.

6.2: Responsibilities of the e-Safeguarding Coordinator

- Promote an awareness and commitment to e-Safeguarding throughout the school.
- Be the first point of contact in school on all e-Safeguarding matters.
- Create and maintain e-Safety policies and procedures, with the support of other members of staff.
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation.
- Ensure that e-Safety education is embedded across the curriculum.
- Ensure that e-Safeguarding is promoted to parents and carers.

- Liaise with appropriate staff in school, the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- Monitor and report on e-Safeguarding issues to the Senior Leadership Team as appropriate.
- Ensure that an e-Safety incident log is kept up to date. This will be done using Cpoms.

6.3: Responsibilities of the Designated Safeguarding Lead

The safeguarding lead should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Unreported monitoring and filtering incidents
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Online-bullying

6.4: Responsibilities of Teachers and Support Staff

- Read, understand and help promote the school's e-Safeguarding policies and guidance.
- Read, understand and adhere to the school's staff Acceptable Use Policy.
- Develop and maintain an awareness of current e-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed e-Safeguarding messages in learning activities where appropriate.
- Supervise and guide pupils carefully when engaged in learning activities involving technology.
- Be aware of what to do if an e-Safety incident occurs and to report any suspected misuse or filtering issues to SLT.
- Pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Maintain a professional level of conduct in personal use of technology at all times.
- In lessons, where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

6.5: Responsibilities of Technical Staff Employed by the Local Authority and Visiting Users

- Read, understand and adhere to the school staff Acceptable Use Policy.
- Report any e-Safety related issues that come to your attention to the e-Safeguarding coordinator or a member of SLT.
- Maintain a professional level of conduct in your personal use of technology at all times.
- Support the school in providing a safe technical infrastructure to support learning and teaching.
- Support the security of the school ICT system.

6.6: Responsibilities of Pupils

- Read, understand and adhere to the school pupil Acceptable Use Policy.
- Help and support the school in the creation of e-Safeguarding policies and practices and to adhere to any policies and practices the school creates.

- Know and understand school policies on the use of mobile phones, digital cameras and handheld devices.
- To know and understand school policies regarding cyber bullying.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in school and at home.
- Understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in school or at home, or if they know of someone who this is happening to.
- To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

6.7: Responsibilities of Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, the school website, social media and information about local and national online safety campaigns. Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines by doing the following:

- Helping and supporting the school in promoting e-Safety.
- To read, understand and promote the school pupil Acceptable Use Policy with their children.
- Take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss e-Safeguarding concerns with their children, show an interest in how they are using technology and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

6.8: Responsibilities of the Governing Body

Governors are responsible for the approval of this Online Safety Policy and for reviewing the effectiveness of the policy. All governors and trustees will receive appropriate safeguarding and child protection training (including online) during their induction. A member of the Governing Body has taken on the role of Online Safety Governor (Julie Palmer). The role of the Online Safety Governor will include:

- Reading, understanding, contributing to and helping promote the school's e-Safeguarding policies and guidance.
- Supporting the work of e-Safeguarding in school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in e-Safeguarding activities.
- Ensuring appropriate funding and resources are available for the school to implement its e-Safeguarding strategy.

7. Education of E-Safety

7.1: Education of Pupils

The education of pupils in online safety is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum will be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of Computing and PHSE and should be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and pastoral activities.
- Pupils should be taught in all lessons to be critically aware of the materials and content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- Staff are encouraged to record any low-level concerns regarding a child's use of the internet to help ensure that early intervention can be carried out when appropriate. Staff will use Cpoms to record and concerns.
- Through R.E and PSHE lessons in upper KS2, children briefly touch upon radicalisation and on how this may look, including how it would look online. This is done in a very child-friendly way and focuses on what actions the children should take if they are to experience it.
- Pupils should be taught what appropriate and inappropriate behaviour looks like when they are online. This should include information about what cyber-bullying is and should include details about what online sexual harassment and up skirting is, as well as the importance of reporting this to a trusted adult if they are to experience it. (See child-on-child abuse Policy for more details.)
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

7.2: Education of Parents/Carers

Many parents and carers play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Regular E-safety newsletters
- The school website
- Parents/carers e-Safety sessions
- High profile events in school E.g. Safer Internet Day

Reference to the relevant web sites/publications

E.g., SWGfL - Safety & Security Online, www.saferinternet.org.uk/, http://www.childnet.com/parents-and-carers

7.3: Education for Staff and Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- Formal online safety training will be made available to staff throughout the year. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive internal online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use Policy.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This online safety policy and its updates will be presented to and discussed by staff in staff/team meetings/training sessions.
- The Online Safety Lead will provide advice and training to individuals as required.

7.4: Education for the Governors

All governors should take part in online safety training and awareness sessions, with particular importance for those who are members of any group involved in online safety and safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority, National Governors' Association or other relevant organisations.
- Participation in school training or information sessions for staff or parents.

8. Technical Equipment, Filtering and Monitoring

The school will be responsible for ensuring that the school's network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities.

Managing the Network and Technical Support:

The school IT technician is responsible for managing the security of the school network and for installing all programmes. All wireless devices are security enabled and only accessible through a secure password. Appropriate settings have been appointed on tablet devices to restrict downloading of apps or in app purchases. All staff members and children have an individual log in and password for devices. All staff members and children are reminded to log out of the school system when leaving a computer or device unattended. Servers, wireless systems and cabling must be securely located and physical access restricted.

Filtering and Monitoring:

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Service Provider and must be reviewed annually (or more if required) and updated in response to changes in technology and patterns of online safety incidents/behaviours.

The school uses the Smoothwall filtering service. Staff should always contact the IT Technician for blocking and unblocking specific websites. The school's designated safeguarding lead (DSL), members of the school's senior leadership team and the governors must work closely with the school's IT service providers in all aspects of filtering and monitoring.

School procedure for reporting breaches of filtering will be shared thoroughly with all members of the school community. If staff or pupils discover unsuitable sites, the URL will be reported to the School Designated Safeguarding Lead and this will then be recorded and escalated as appropriate. To report a website staff should use Cpoms and incidents should be reported by clicking on the 'Online Safety' category. All changes to the school filtering policy will be logged and recorded by the Designated Safeguarding Lead.

The Leadership Team will ensure that regular checks are made to ensure that the filtering methods selected are effective and appropriate. Checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader, the Designated Safeguarding Lead and a governor. Any material that the school believes is illegal will be reported to appropriate agencies such as the police or to Child Exploitation and Online Protection Command (CEOP) immediately.

A review of filtering and monitoring will be carried out regularly by the SLT to identify the school's current provision, any gaps, and if it meets the specific needs of the school's pupils and staff. The risk profile of our school's pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL) should be considered. When checking filtering and monitoring systems it is important to check a range of school owned devices and services, including those used off site as well

as a range of user groups. All checks and reviews of the filtering and monitoring system must be logged and should include;

• When the checks took place.

• Who did the check.

• Resulting actions.

Additional Filtering and Monitoring:

- All users will have clearly defined access rights to the school's technical systems and devices.
- All users will be provided with a username and secure password for regular used online resources and there will be a record of users and their usernames kept safely in school/on an online document.
- All users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- When pupils have finished using a school device they must ensure that they not only log off of the device but that they remove their account from the device also.
- Internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored.
- Internet filtering and monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices provided by the school are protected by up to date virus software.
- An agreed policy is in place the provision of temporary access of supply teachers/guests onto the school systems.
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on school devices. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.
- The Headteacher is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.

9. Mobile Technologies

Mobile technology devices may be school owned, provided or personally owned and might include: smartphones, tablets, laptops or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud-based services such as email and data storage.

All users should understand that the primary purpose of the use mobile and personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education program.

The school's Acceptable Use Policy (AUP) for staff, pupils and parents/carers will give consideration to the use of mobile technologies. This is signed by all new members of staff as part of their induction process.

10. Managing digital content

10.1 Using Images, Video and Sound

- Written permission from parents or carers will be obtained for the following locations before photographs of pupils are published. This will be done annually or as part of the home-school agreement on entry to the school.

    - On the school's website or blog
    - On the school's learning platform
    - In the school prospectus and other printed promotional material
    - In display material that may be used around the school
    - In display material that may be used off site
    - Recorded or transmitted on a video or via webcam in an educational conference

- Parents and carers may withdraw permission, in writing, at any time.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, using, sharing, the publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet.
- Digital images, videos and sounds will only be created using equipment provided by the school or a safe and reliable source.
- Staff and pupils will follow the school policy on creating, using and storing digital resources.
- In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file name or in accompanying text online; such resources will not be published online without the permission of the staff and pupils involved
- Pupils' full names will not be used anywhere on a website or blog without full parental permission.
- Pupils must not take, share or publish images of others without their permission.

10.2 Storage of Images

- Any images, videos or sound clips of pupils must be stored on the school network and never transferred to personally-owned equipment.
- Pupils and staff are not permitted to use personal portable media for storage of any images, videos or sound clips of pupils.

11. Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, schools are likely to be subject to greater scrutiny in their care and use of personal data.

Therefore, personal data will be recorded, processed, transferred and made available according to the current data protection legislation. The school will ensure that:

- It has a Data Protection Policy which includes all the necessary information (See Howden Junior School Data Protection Policy for more detail).
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- It has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO).
- It has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest.
- ICT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom.
- It has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- It understands how to share data lawfully and safely with other relevant data controllers.
- It reports any relevant breaches to the Information Commissioner within 72 hours of becoming aware of the breach in accordance with UK data protection law.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.
- When children leave the school, the DSL will ensure that the child's data and child protection files are transferred to the child's new school within 5 days for an in-year transfer and within the first 5 days of the start of a new term when the school is closed. This allows the new setting to have support in place for when the child arrives.

When personal data is stored on any mobile device or removable media the:

- Data must be encrypted and password protected.
- Devices must be password protected.
- Devices must be protected by up to date virus and malware checking software.
- Data must be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected.
- Will not transfer any school personal data to personal devices except as in line with school policy.
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

12. Managing ICT Systems and Access

- The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
- Servers and other key hardware or infrastructure will be located securely.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- Virus protection is installed on all appropriate hardware, and will be kept active and up to date.
- The school will agree which users should and should not have internet access, and the appropriate level of access and supervision they should receive.
- All users will sign an Acceptable Use Policy provided by the school, appropriate to their age and type of access. Users will be made aware that they must take responsibility for their use and behaviour while using the school ICT systems and that such activity will be monitored and checked. This includes all staff and children.
- Pupils will access the internet using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow pupils to access the internet through their ID and password. Members of staff will abide by the school AUP at all times. They will not allow children unsupervised access to their computers.
- Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff.
- The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.
- The school will regularly audit ICT use to establish if the e-Safety policy is adequate and that the implementation of the e-Safety policy is appropriate. We will regularly review our internet access provision, and review new methods to identify, assess and minimise risks.

13. Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before their use in school is allowed.

- Emerging technologies can incorporate software and/or hardware products.
- The school will periodically review which technologies are available within school for any security vulnerabilities that may have been discovered since deployment.
- The acceptable use of any new or emerging technologies in use within school will be reflected within the school e-Safeguarding and Acceptable Use policies.
- Prior to deploying any new technologies within school, staff and pupils will have appropriate awareness training regarding safe usage and any associated risks.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- The sending of abusive or inappropriate text, picture or video messages is forbidden.
- Staff will not upload any personal information or content to any school accounts, including Google Suite for Education and school blogs. Staff will ensure that if they use their own personal devices to connect to these systems, their devices will not link to the account and make any automatic updates/uploads.
- When using Google Suite for Education, the e-mail and chat functions will be disabled for children. Children will only be able to use the service if we have had permission gained from parents/guardians.
- Children will share all files created in Google Suite for Education with their teacher. Hapara will do this automatically.
- When using Chromebooks, children must login using their own account details, so that their activity can be tracked.

14. Email

- Staff and pupils should use approved email accounts allocated to them by the school and should be aware that any use of the school email system will be monitored and checked.
- Pupils may only use school-provided email accounts for school purposes and only under direct teacher supervision for educational purposes.
- Pupils are not permitted to access personal e-mail accounts during school.
- Responsible use of personal web mail accounts by staff is permitted.
- School email accounts should be the only account that is used for school-related business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- Pupils and staff will be reminded when using email about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.
- Any inappropriate use of the school email system or receipt of any inappropriate messages from another user should be reported to a member of SLT immediately.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school-headed paper.
- Teaching staff may also use ClassDojo messaging to contact parents, who have signed up voluntarily, but should ensure all messages are appropriate.

15. Using Blogs, Wikis, Podcasts and other ways for Pupils to Publish Content Online

- Blogging, podcasting and other publishing of online content by pupils will take place only on the school website.
- Pupils will not be allowed to post or create content on sites unless the site has been approved by a member of the teaching staff.
- Any public blogs run by staff on behalf of the school will be hosted on the learning platform/school website/YHGfL blog and postings should be approved by the head teacher before publishing.
- Teachers will model safe and responsible behaviour in their creation and publishing of online content within the school learning platform. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
- Pupils will not use their real name when creating publicly-accessible resources. They will be encouraged to create an appropriate nickname.
- Personal publishing will be taught via age-appropriate sites that are suitable for educational purposes. They will be moderated by the school where possible.
- Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, wikis, and other online publishing outside school.
- Material published by pupils, governors or staff in a social context which is considered to bring the school into disrepute or considered harmful to, or harassment of another pupil or member of the school community will be considered a breach of school discipline and treated accordingly.

16. Social Media

The school uses social media accounts to complement the existing communication methods with parents and the local community. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school when using social media through:

- Ensuring that personal information is not published.
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions.
- Risk assessment, including legal risk (HJS Social media account risk assessment).
- No reference should be made in social media to pupils, staff or parents without permission.
- Staff must not engage in online discussion on personal matters relating to members of the school community and personal opinions should not be attributed to the school or local authority. Staff should not make links or mentions to HJS on their personal social media accounts.
- Security settings on personal social media profiles are regularly checked by the person responsible to minimise risk of loss of personal information.

The school's official social media account has:

- A clear process for the administration and monitoring of these accounts – involving at least two members of staff (Executive Head and Head of School). The HT is overall responsible for the school's social media accounts.
- A code of behaviour for users of the accounts (see Acceptable Use Policy 24-26 for more details).
- Systems for reporting and dealing with abuse and misuse.
- They should be used for educational purposes only.

Personal Use:

- Personal communications, which do not refer to or impact upon the school, are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- The school permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

- As part of active social media engagement, the school will carry out a weekly check of its social media accounts. This will be carried out by the SBM. This will be to check for hacking, spam, inappropriate accounts or comments linked with the school and to uphold the school's reputation.

For more detail around the school's social media use see Social Media (Official School Facebook/X) Policy.

17. Mobile Phone Usage and Social Media Usage by children:

17.1 General Issues

- Mobile phones and personally-owned devices will not be used in any way during lessons or formal school time, unless for a reasonable purpose.
- Use of mobile phones on school premises by pupils is not permitted, and all mobile phones and personally-owned devices will be handed in at reception, or to the class teacher, should they be brought into school.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.
- As stated in KCSIE 2024, all staff must be aware of children using mobile phones to carry out child-on-child abuse, sexting, online sexual harassment including sexual comments and jokes online. They must also be aware of children using mobile phones for up-skirting which is the act of taking a picture under a person's clothing without them knowing with the intention of viewing their genitals or buttocks to obtain sexual gratification or to cause the victim humiliation. (See Child-on-Child Abuse Policy 2024 for more details).
- Staff must also be aware of cyber-bullying in and out of school. This is defined as the use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature. Should cyber-bullying be identified to have taken place by a child, it will be dealt with using the school's behaviour policy (See Behaviour Policy 2024 for more details).

18. Data Protection and Information Security

- The school community will act and carry out its duty of care for the information assets it holds in line with its Data Protection Act 1998 commitments.
- All computers that are used to access sensitive information should be locked when unattended.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- Staff and pupils will not leave personal and sensitive printed documents on printers or within public areas of the school.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the school's information-handling procedures and, for example, not left in cars or insecure locations.
- Where personal information needs to be taken off site (in paper or electronic form) this will be kept secure when not in use.

18.1 Dealing with unsuitable and inappropriate activities

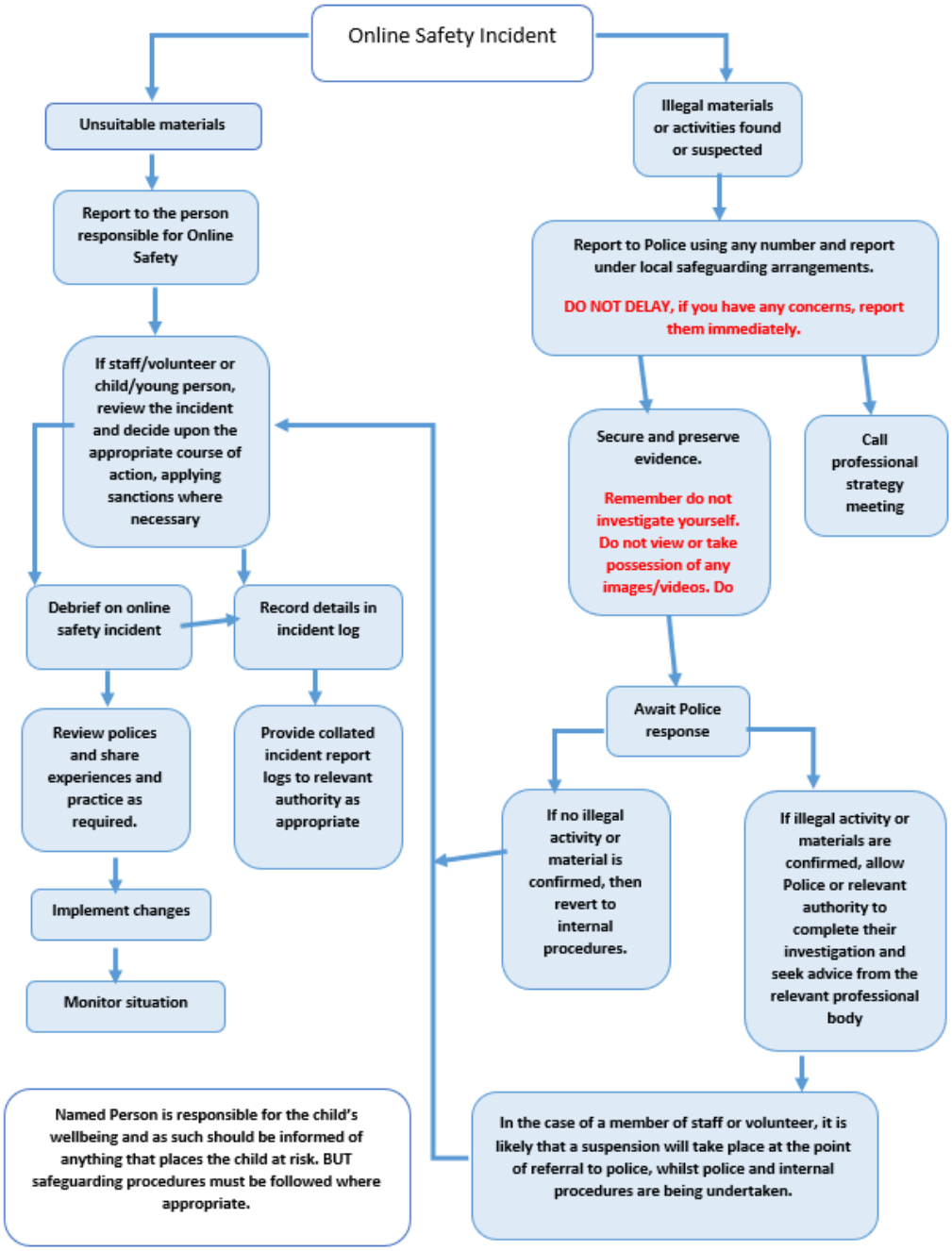
The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in or outside the school when using school equipment or systems. The school's policy restricts usage as follows:

		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act: • Gaining unauthorised access to school networks, data and files, through the use of computers/devices						X

• Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school/academy				X	
Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)				X	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				X	
Using school systems to run a private business				X	
Infringing copyright				X	
On-line gaming (non-educational)				X	
On-line gambling				X	
On-line shopping (not-related to school)				X	
File sharing			X		
Use of social media			X		
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube			X		

18.2 Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the flowchart below for responding to online safety incidents and report immediately to the police.



18.3 Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place through careless and irresponsible use or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required following the school's normal behaviour/disciplinary procedures.

If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Staff must be aware of the requirement for children to have an appropriate adult with them at all times during any police investigation. The is adult is to support, advise and assist the child. The computer should be isolated.

19. Management of Assets

- Details of all school-owned hardware will be recorded in a hardware inventory.
- Details of all school-owned software will be recorded in a software inventory.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Any incidents or failure to comply with this policy and also the Acceptable Use Policies will be dealt with following the school's normal behaviour or disciplinary procedures. Discipline consequences will be at discretion of the Headteacher.

Instances of **cyberbullying** will be taken very seriously by the school and dealt with using the school's anti-bullying procedures. The school recognises that staff as well as pupils may be victims and will take appropriate action in either situation.

POLICY APPROVED BY THE GOVERNING BODY ON September 2024

POLICY DUE FOR RENEWAL ON September 2025