



Heatherley Primary School

Online Safety

Online Safety Lead: Tyler Lieber and Sean Kavanagh

E-Safety and Acceptable Use Policy

Introduction

The internet has undeniably become an integral part of our lives. Many people rely on the internet or internet services for daily tasks, making it an essential element in our increasingly technological world. The internet and its applications have a profound impact on all aspects of life, including education, business, and social interactions. In schools, the internet is extensively used by both staff and children during instructional sessions. It is the duty and responsibility of all staff members to ensure that children use the internet safely and responsibly and understand the importance of e-safety and how to apply it in situations outside of school. The Computing Subject Leader is responsible for ensuring that all staff are aware of our E-Safety Policy and receive regular updates on its content.

Scope of the policy

This policy applies to all members of the school community, including staff, pupils, governors, volunteers, parents/carers, visitors, and community users who have access to and use the school's ICT systems, both on and off school premises. The Education and Inspections Act 2006 grants Head Teachers the authority, within reasonable limits, to regulate pupils' behaviour off the school site and allows staff to impose disciplinary measures for inappropriate behaviour. This is relevant to incidents of cyberbullying or other e-safety issues addressed by this policy that occur outside the school but are connected to school membership. The 2011 Education Act expanded these powers to include searching electronic devices and deleting data. Actions can only be taken for issues covered by our current behaviour policy. The school will address such incidents in accordance with this policy and the associated Behaviour and Anti-Bullying policies and will inform parents/carers of known instances of inappropriate e-safety behaviour that occur outside of school.

Roles and Responsibilities:

Governors:

The Governors hold the ultimate responsibility for approving the E-Safety Policy and for regularly reviewing its effectiveness to ensure it meets the necessary standards and remains up to date with current practices and threats. As the Chair of Governors and the Safeguarding governor, Mrs. Gemma Koch plays a crucial role in this process. Her responsibilities include:

1. **Policy Approval:** Mrs. Koch, along with the other Governors, must review and approve the E-Safety Policy, ensuring it aligns with legal requirements and best practices.
2. **Regular Review:** She is responsible for the ongoing evaluation of the policy's effectiveness. This involves assessing whether the policy is being implemented correctly and making necessary adjustments.
3. **Safeguarding Oversight:** As the Safeguarding governor, Mrs. Koch ensures that all aspects of the policy are designed to protect children and staff from online risks.
4. **Monitoring Compliance:** She oversees the adherence to the policy, ensuring that the school's procedures and protocols are being followed appropriately.
5. **Training and Awareness:** Mrs. Koch may also be involved in promoting e-safety training and awareness among staff, children, and parents to ensure everyone understands their role in maintaining a safe online environment.

Her leadership is essential in fostering a secure and supportive online environment within the school.

Headteacher/Head of School: (Mrs James)

- The Head Teacher/Head of School has a duty of care to ensure the safety of all members of the school community, including e-safety. However, the day-to-day responsibility for e-safety is delegated to the Computing Lead.
- The Head Teacher/Head of School (Designated Safeguarding Lead) and other designated safeguarding staff are familiar with the procedures to follow if a serious e-safety allegation is made against a staff member or pupil.
- The Head Teacher regularly monitors devices and ICT use in school which allows us to identify any potential issues early on and implement appropriate measures to address them, ultimately fostering a positive and productive digital learning environment for all.

Heatherley Primary School Computing Lead: (Mr. Sean Kavanagh)

- Takes daily responsibility for e-safety issues and plays a key role in establishing and reviewing the school's computing and e-safety policies.

- Ensures all staff are informed of the procedures to follow in the event of an e-safety incident.
- Provides training and advice to staff.
- Collaborates with school technical staff.
- Receives reports of e-safety incidents and maintains a log of these incidents to guide future e-safety developments. •

Reports regularly to the Head Teacher/Head of School.

Child Protection / Safeguarding Designated Person(s):

The Child Protection/Safeguarding Designated Person(s) is/are trained in e-safety issues and is/are aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data.
- access to inappropriate or illegal materials.
- inappropriate on-line contact with adults, strangers in potential or actual incidents of grooming.
- cyber-bullying.

Technical staff:

Technical staff contracted to support the school with ICT and computing are responsible for ensuring:

- The school's technical infrastructure is secure and protected against misuse or malicious attacks.
- Access to the networks and devices is restricted through a strictly enforced password protection policy, requiring regular password updates.
- Regular updates and applications of filtering systems.

- Staying informed about the latest e-safety technical information to effectively fulfill their e-safety responsibilities and update others as needed.
- Regular monitoring of network, internet, remote access, and email usage to identify and report any misuse or attempted misuse to the Head of School/Head Teacher for further investigation and action.
- Implementation and regular updates of monitoring software/systems as specified in school policies.

Teaching and Support Staff:

All teaching and support staff are responsible for ensuring that:

- They maintain an up-to-date awareness of e-safety matters and the current school online safety policy and procedures.
- They have read and understood the Staff Acceptable Use Policy/Agreement (AUP).
- They report any suspected misuse or problems to the Head of School/Head Teacher/Computing Lead for investigation, action, or sanction.
- All digital communications with pupils, parents, and carers are conducted professionally and follow the agreed school procedures.
- E-safety awareness is integrated into all aspects of the curriculum and other activities and is regularly reinforced.
- Pupils understand and adhere to the e-safety and acceptable use policies.
- Pupils possess strong research skills and understand the importance of avoiding plagiarism and respecting copyright regulations.
- They monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities, ensuring compliance with current policies.
- In lessons where internet use is pre-planned, pupils are guided to appropriate websites, and processes are in place for handling any unsuitable material encountered during internet searches.
- All pupils know the appropriate actions to take if they encounter something concerning, such as a pop-up or communication from an unknown source.
- Concerns to be logged on CPOMS

Pupils:

- are responsible for using the school digital technology systems in accordance with the Pupil Acceptable Use Policy.
- should possess strong research skills, recognise the importance of avoiding plagiarism, and respect copyright laws.
- must understand the significance of reporting any abuse, misuse, or access to inappropriate materials, and be aware of the procedures for doing so.
- are expected to be familiar with and understand the policies regarding the use of mobile devices and digital cameras, including the guidelines for taking and using images and addressing cyber-bullying.
- should recognise the importance of practicing good e-safety when using digital technologies outside of school, understanding that the school's E-Safety Policy extends to their actions outside of school if they pertain to their association with the school.
- should get in external agencies if needed for support

Parents / Carers:

Parents and carers play a vital role in ensuring their children use the internet and mobile devices appropriately. The school will actively support parents in understanding these issues through various channels, including parents' evenings, newsletters, our website, and information about e-safety campaigns. We encourage parents and carers to support the school in promoting good e-safety practices and to adhere to the following guidelines:

- Use of digital and video images taken at school events for example not sharing these images on social media if the image or video includes other pupils.
- Access to parents' sections of the website.
- Use of their children's personal devices within the school (where permitted).

Teaching and Learning - Use of the Internet

Heatherley Primary School is dedicated to embracing evolving technology and offering our children a high quality computing curriculum as part of their educational journey. This naturally includes utilising the internet for various purposes. Children will be taught how to use the internet safely and effectively, employing it efficiently for tasks such as information retrieval, coding, programming, and using enhancement or manipulation tools.

Internet usage is a crucial part of the curriculum and an essential learning tool for both staff and children. Meaningful and purposeful internet use can elevate educational standards, boost children achievement, support the professional activities of staff, enhance the school's management, information, and business administration systems, and foster immediate lines of communication and inquiry.

Given that the Internet is inherently not an externally managed resource, it is vital to have appropriate measures in place to limit access to inappropriate content. Additionally, all children and staff must be fully prepared and supported to use technologies responsibly and safely.

Our Aims

The objective of this policy is to guarantee that children possess the necessary knowledge and competencies for both in-school and out-of-school settings. It is imperative that children have the chance to develop skills in evaluating and handling potential risks independently. Equally crucial is providing staff with consistent E-Safety training and keeping them updated on current practices. Additionally, we have a responsibility to our parents, offering annual E-Safety workshops and providing immediate access to E-Safety resources through our website.

Assessing Risks

Heatherley Primary will take reasonable precautions to prevent access to inappropriate material on the internet through all mobile devices. School recognises that there are a number of potential risks including,

- Loss of privacy

- Sexting
- Exposure to offensive / inappropriate materials
- Infection by malware, viruses and spyware
- Radicalisation through the use of social media and the internet

The school ICT operating system security will be reviewed regularly in order to minimise potential risks occurring.

Heatherley Primary school is taking proactive measures to minimize children's exposure to potentially harmful content online. Collaborating closely with the IT Support company, the school's governing body and Designated Safeguarding Lead (DSL) to ensure the implementation of suitable filters and monitoring systems. The filtering software providers are affiliated with the Internet Watch Foundation, ensuring compliance with the Children's Internet Protection Act. This software effectively blocks access to inappropriate web content, including but not limited to terrorism, child sexual abuse, and adult materials. Monitoring systems are in place to promptly notify the IT support team of any flagged content. Additionally, where necessary, physical monitoring of children's online activities is conducted. Regular checks of filtering and monitoring systems are performed on a termly basis across various devices and locations within the school premises. The school ensures that filtering aligns with the needs of its children, considering their age and other relevant factors, utilising resources such as the IWF's URL list and guidance from the Home Office/Prevent Duty. In case of any concerns raised by the systems, appropriate actions are promptly taken by the IT support team.

Ensuring online safety encompasses more than just internet use; it extends to all wireless electronic devices such as mobile phones, gaming consoles, cameras, tablets, and webcams. With the growing accessibility of digital technology through these devices, it's crucial to acknowledge that safety concerns stem not from the technology itself but from how it's used. Consequently, educational institutions must ensure that young individuals can utilise the internet and related communication technologies appropriately and securely. According to Ofsted, technology presents limitless possibilities and is continually advancing, with access becoming increasingly universal and mobile. As

such, schools must be well-versed in the common risks and challenges associated with technology use to effectively safeguard their children.

Risks for Children in the Digital Environment						
Risk Categories	Content Risks		Conduct Risks	Contact Risks		Consumer Risks
Cross-cutting Risks	Privacy Risks (Interpersonal, Institutional & Commercial)					
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)					
	Risks on Health & Wellbeing					
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters		Marketing Risks	
	Harmful Content	Harmful Behaviour	Harmful Encounters		Commercial Profiling Risks	
	Illegal Content	Illegal Behaviour	Illegal Encounters		Financial Risks	
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters		Security Risks	

Above identifies the The OECD risks for children in the digital environment.

The 4C's classification of online risks identify that:

1. **Content:** This refers to the material that students may come across while using the internet. It includes inappropriate or harmful content such as violence, explicit material, misinformation, or content promoting harmful behaviors like self-harm or substance abuse. Monitoring and filtering tools can help limit exposure to such content, while educating students about critical thinking and digital literacy skills empowers them to navigate online content responsibly.
2. **Contact:** Contact risks involve interactions with other users online, including strangers or peers. This can include cyberbullying, grooming by predators, or exposure to inappropriate communication. Teaching students about online safety, privacy settings, and the importance of reporting any concerning interactions can help mitigate contact risks. Additionally, fostering open communication channels between students, educators, and parents encourages students to seek help when needed.
3. **Conduct:** Conduct risks pertain to students' own behaviour online, including cyberbullying, harassment, or engaging in illegal activities. Educating students about digital citizenship and responsible online behaviour is essential in

addressing conduct risks. Emphasizing the importance of empathy, respect, and ethical behaviour in all online interactions helps create a positive and inclusive online environment.

4. **Commercialism:** Commercialism risks involve exposure to advertising, marketing tactics, and online scams. Students may encounter targeted advertisements, sponsored content, or deceptive marketing practices that can influence their behaviour or compromise their privacy. Educators should educate students about online advertising tactics, privacy policies, and strategies to protect their personal information from exploitation by advertisers and scammers.

By addressing the 4 C's—content, contact, conduct, and commercialism—through education, awareness, and proactive measures, schools can empower children to navigate the online world safely and responsibly.

Communications

Here are the guidelines for utilising communication technologies within the school setting:

- The school's official email service is considered secure and is monitored. Users should be aware that email communications are subject to monitoring.
- Users are required to promptly report any communication that causes discomfort, is offensive, discriminatory, threatening, or indicative of bullying to the Head of School or Head Teacher, in accordance with school policy. Under no circumstances should they engage with such communication.
- All digital communication between staff and pupils or parents/carers (including emails, social media interactions and chats) must maintain a professional tone and content. Such communication should exclusively occur on monitored school systems; personal email addresses, text messaging, or social media platforms are not to be used for these exchanges.
- Throughout the school, whole class email addresses are utilized, supplemented by individual school email addresses for educational purposes.
- Children should receive education on online safety, including the risks associated with sharing personal information. They should also be equipped with strategies to handle inappropriate communications and reminded to communicate responsibly when utilising digital technologies.

- Personal information will not be posted on the school website and only official email addresses should be used to identify members of staff.

Email, Webcam use and Blogging

Our staff strictly adhere to a code of conduct that prohibits them from sharing personal contact details with parents or children. Any communication, whether via email or other platforms, should be routed through the school office for appropriate handling. We emphasise to both children and staff the importance of safeguarding usernames and passwords. Additionally, video conferencing and webcam usage are implemented with age-appropriate supervision for our children.

The Heatherley Primary website is accessible to everyone without requiring a username or password. The Computing Lead oversees site monitoring, while staff members manage their respective class pages. It is the responsibility of all users to ensure that appropriate content is uploaded. Should any inappropriate material appear, it must be promptly reported to the Head of School for appropriate action.

Parents provide yearly permission, as part of the Admission to School Pack, for the posting of photographs and videos of their child on the website. Staff are required to refrain from associating pupil names with photographs and must obtain permission before publishing any content.

Teaching of E-safety

At Heatherley Primary, E-Safety is integrated into our computing curriculum across all year groups, where children learn:

- The SMART code of conduct.
- Never to disclose personal details.
- Not to share passwords except with a teacher or parent/carer.
- Not to engage in cyber-bullying.
- Never to agree to meet online acquaintances in person.
- To visit only trusted and supervised websites.
- To assess the credibility of websites for relevant information.

- To promptly inform an adult upon encountering inappropriate content by closing the device or screen and seeking guidance.
- To confide in a trusted adult if they feel frightened or uncomfortable online.
- To only accept friend requests from individuals they know in real life.
- To use avatars instead of personal profiles.

At Heatherley Primary, we prioritise safety on social networking sites by educating all stakeholders, including parents, about safe usage practices. We carefully select and obtain parental consent for photographs of children to minimise misuse risks, ensuring that full names are never used alongside these images online. Additionally, we inform all system users about the monitoring of network and internet activities.

Every staff member receives and understands our comprehensive E-Safety policy, with access to ongoing training. E-Safety is integrated into our curriculum, with safe internet rules prominently displayed in classrooms and regularly reinforced. We assess emerging technologies for educational benefits before implementing them.

Removable media is prohibited unless absolutely necessary and approved after virus scanning. Personal data handling complies with the Data Protection Act, and staff are accountable for all issued equipment. Images of children are not stored on staff personal devices, and all user credentials are confidential.

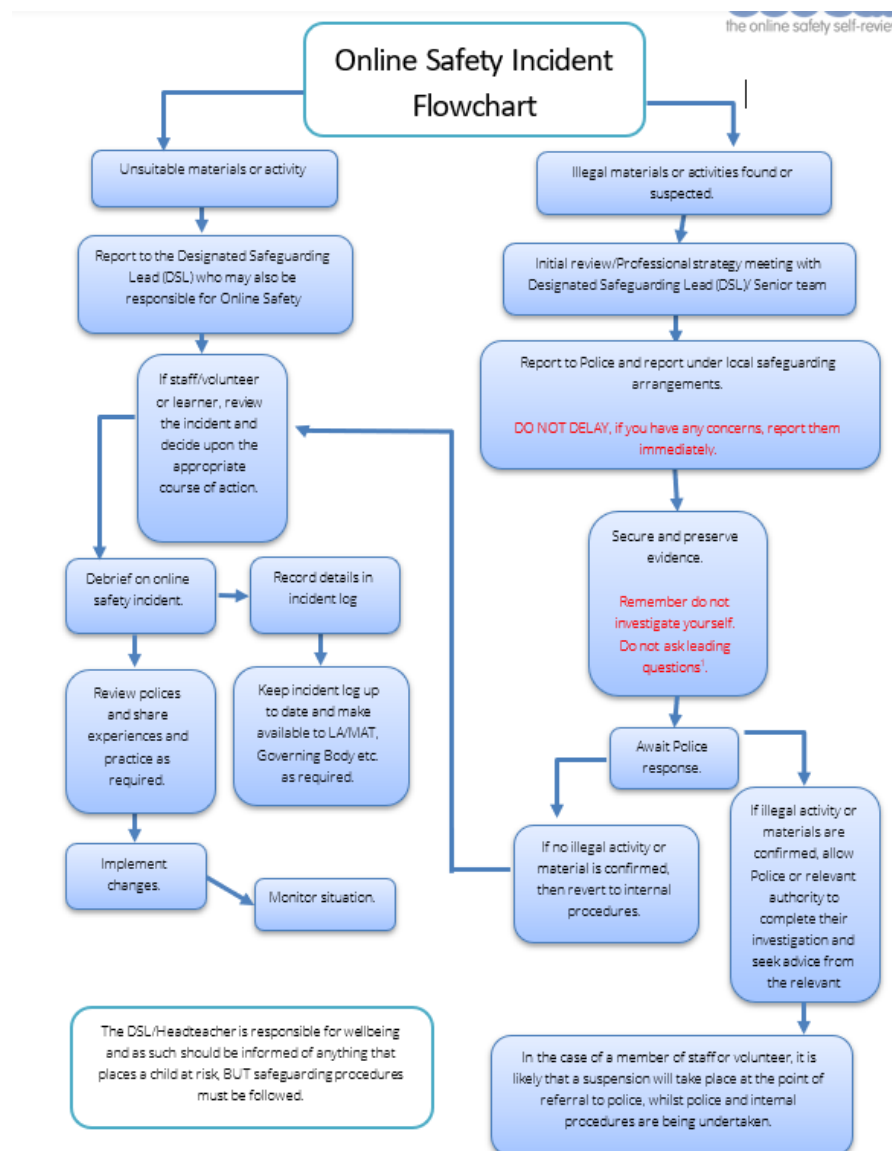
Staff emails are kept private, with contact directed through official channels. Confidential materials are encrypted and stored on the school's password-protected server. USB drives require permission and encryption, and any lost or stolen items with sensitive data are reported to the child protection officer promptly. Regular updates maintain virus protection.

Reporting of E-Safety Incidents

All E-Safety incidents will be directed to the Computing Lead, who will conduct investigations and document the incident on CPOMs (refer to flowchart below). Subsequently, the incident will be reported to the Class Teacher and/or the Child Protection/Safeguarding Lead, depending on its nature. Parents/Carers will receive relevant notifications as needed.

This policy is applicable to the entire school community, including the Senior Leadership Team, school Governors, staff, and children. It aligns with other policies such as Safeguarding, Behaviour, and Anti-Bullying.

The flowchart below is available to staff to support the decision-making process for dealing with online safety incidents:



General Data Protection Regulations (GDPR)

Heatherley Primary fully complies with information legislation. For the full details on how we use children's personal information, please refer to the Data Protection section on the school website www.heatherleyprimaryschool.co.uk

Parent/Carers consent form and E-Safety Rules

At Heatherley Primary all pupils will have access to the school's computer facilities including the internet as an essential part of learning, as required by the National Curriculum. Both pupils and their parents/carers are asked to sign to show that the e-safety rules have been understood and agreed.

Pupils Name: _____

Parent/Carer Name: _____

- As the parent or legal guardian of the above pupil, I have read and understood the attached school rules and now grant permission for my son/daughter to use the internet and other Computing Science facilities at School.
- I know that my son/daughter has signed an E-Safety Agreement and they have a copy of the school E-Safety rules.
- We have discussed this document and they agree to follow the rules to support the safe and responsible use of the internet and other technologies at Heatherley Primary School.
- I accept that the school cannot be held responsible for the nature and content of materials accessed through the internet and mobile technologies, but I understand that they will take every reasonable precaution to keep pupils safe and to prevent pupils accessing inappropriate materials.
- The school has an educationally filtered service, restricted access email and provides age appropriate teaching around internet use and E-Safety issues.
- I will support the school by promoting safe use of the internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.
- I understand that these rules are designed to keep my child safe and that any irresponsible behaviour on the part of my son/daughter may result in sanctions being applied.

Parents Signature: _____ Date: _____

Please complete and return to the school office.



Pupil Acceptable Use Agreement Pupil Acceptable Use Policy Agreement- for younger pupils (Foundation/KSI)

SMART Rules:

- * Always seek permission from a teacher or responsible adult before using computers or tablets.
- * Only engage in activities approved or recommended by a teacher or responsible adult.
- * Handle computer equipment with care and respect.
- * Don't hesitate to ask for assistance from a teacher or responsible adult if uncertain about what to do or if something seems wrong.
- * Immediately report anything upsetting seen on the screen to a teacher or responsible adult.
- * Understand that breaking the rules may result in losing computer or tablet privileges.

Signed (child): _____

Signed (parent): _____



Pupil Acceptable Use Agreement Pupil Acceptable Use Policy Agreement- for Key Stage Two School policy

Acceptable Use Agreement

SMART Rules:

We acknowledge the significant role of digital technologies such as computers, tablets, phones, and gaming systems in our lives, both within and outside school. These tools offer immense opportunities for learning, creativity, and exploration of the world around us. However, with this privilege comes the responsibility to ensure our safety and the security of the systems and fellow users. By using technology, we assert our entitlement to a safe experience.

For Personal Safety:

- We understand that the school may monitor our usage of systems, devices, and digital communications.
- We commit to safeguarding our usernames and passwords, refraining from sharing them or attempting to use others'.
- We remain vigilant of potential risks associated with online interactions, exercising caution with unfamiliar individuals.
- We refrain from disclosing personal information, such as names, addresses, or contact details, online.
- In the event of arranging offline meetings with online acquaintances, we pledge to do so in public settings and with the accompaniment of a trusted adult.
- We undertake to promptly report any encounter with unpleasant or inappropriate content or messages online.

Equal Rights and Responsibilities:

- We recognise the educational purpose of school systems and agree to use them, accordingly, seeking permission for personal or recreational use.
- We refrain from actions that may disrupt internet capacity or hinder others' work progress without authorisation.
- We seek permission from staff before engaging in online gaming or video broadcasting activities.
- We pledge to respect the work and property of others, refraining from unauthorized access or alteration of their files.
- We commit to respectful and responsible communication, refraining from using offensive language and acknowledging diverse viewpoints.
- We agree not to capture or distribute images of others without their consent.
- We pledge to report any equipment or software damage or faults promptly, regardless of the cause.

Internet Usage Guidelines:

- We acknowledge the importance of seeking permission to use others' original work and respect copyright protections.
- We agree not to download copyrighted material, including music and videos.
- We understand the need to verify the accuracy of information found online, recognising the potential for misinformation.

Accountability:

- We acknowledge our responsibility for our actions, both within and outside school premises.
- We understand that the school reserves the right to address incidents of inappropriate behaviour, even if they occur outside school grounds but involve our association with the school community.
- We acknowledge that failure to adhere to this agreement may result in disciplinary measures.

Pupil Acceptable Use Agreement Form:

I confirm that I have read, understood, and agree to accept by the rules outlined in the Acceptable Use Agreement.

Name of Pupil: _____ Class: _____

Signed: _____ Date: _____