Hagley Primary School

Online Safety Policy

Date: **September 2025**

Date of review: **September 2026**

Responsible member of staff: **Mrs Sarah Watkins**

Signature:

(*Chair of Governors*)

Signature:

(*Head Teacher*)

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even truer for children, who are generally much more open to developing technologies than many adults. This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy sets out how we educate children about the potential risks.

Aims

Hagley Primary School will:

Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors

Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology

Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Ensure that school has robust filtering and monitoring systems and processes in place in line with KCSIE 2025.

Ensure that all staff receive appropriate safeguarding and child protection training, including online safety which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring as part of their induction. (KCSiE 2025)

Ensure all staff and governors receive regular safeguarding and child protection updates including Online Safety and cyber security

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying

cyber-bullying: advice for headteachers and school staff

Relationships and sex education

Searching, screening and confiscation

Meeting digital and technology standards in schools and colleges Sharing nudes and semi nudes

It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

We are aware that, technology, and risks and harms related to it, evolve and change rapidly. Hagley Primary School Primary School will therefore carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. We will continue to use the online safety self-review tool for schools (360 safe Audit) in order to do this.

3. Roles and responsibilities

3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff namely the DSL and Online Safety Leader, Sarah Watkins, to discuss online safety, and monitor online safety logs.

The governor who oversees online safety is Adam Tyler.

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on the school's Acceptable Use Policy
- Ensure all staff undertake appropriate online safety and cyber security training
- Ensure that the online safety and computing curriculum teaches children to effectively keep themselves and others safe online
- Ensure sufficient resources are available through effective budget planning to keep the school network infrastructure, filtering and monitoring up to date
- Ensure that, as part of the requirement for staff and children to undergo regular updated safeguarding training, including in relation to online safety, that safeguarding training for staff, including online safety training, is integrated, aligned and considered as part of the whole school safeguarding approach and wider staff training and curriculum planning. (KCSiE 2025)

3.2 The Headteacher

The Headteacher (Vanessa Payne) has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Online Safety Lead, Sarah Watkins.

The Headteacher and Senior Leaders are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues.

The Headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead (DSL) and Online Safety Lead

The DSLs will support the Online Safety Leader who will take a lead responsibility for online safety in school, in particular by:

- Ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, network managers and other staff, as necessary, to address any online safety issues or incidents
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged appropriately and dealt with in line with the school behaviour policy and safeguarding procedures
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Understand the filtering and monitoring systems and processes in place

This list is not intended to be exhaustive.

3.4 The Online Safety Lead

Sarah Watkins is Hagley Primary School's named Online Safety Leader. Her responsibilities include that she:

- has a leading role in establishing and reviewing the school online safety policies/documents with support and guidance from DSLs
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- provides training and advice for staff, including when patterns of incidents occur
- liaises with the Local Authority and / or other relevant body
- receives communication about online safety incidents to inform future online safety developments
- meets regularly with the Governors to discuss current issues and curriculum development.

3.5 The Network manager / School Business Manager

Hagley Primary School Primary school use Chestnut Infrastructure/Entrust as their Network Managers.

The network managers are responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents that they discover are logged and dealt with appropriately in line with this policy
- Users may only access the networks and devices through a properly enforced password protection

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and volunteers are responsible for:

- Maintaining an understanding of this policy
- Reporting any suspected misuse or problem to the Online Safety Lead and DSL
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use
- Working with the Online Safety Lead and DSLs to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school safeguarding policy

This list is not intended to be exhaustive.

3.7 Parents

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? - UK Safer Internet Centre
- Help and advice - Childnet International

- Parent resource sheet - Childnet International
- Support around the consensual and non-consensual sharing of nudes and semi-nudes (previously referred to as sexting) – internetmatters.org

Hagley Primary School will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national/local online safety campaigns/literature.

https://hagleyprimary.org.uk/online-safety/

3.8 Visitors and members of the community

Visitors and members of the community, who use the school's ICT systems or internet, will be made aware of this policy, when relevant, and expected to read and follow it. They will be expected to agree to the terms on acceptable use before they are able to sign onto the network.

4. Educating pupils about online safety

As written in KCSiE 2025: It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and

escalate any concerns where appropriate. The education of pupils in online safety/computing 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 including through PHSE which includes aspects about online safety.

As it states in Keeping Children Safe in Education, the breadth of issues associated with online safety is considerable, but can be categorised into four main areas:

• **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, misinformation, disinformation, conspiracy theories, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce -** risks such as online gambling, inappropriate advertising, phishing and or financial scams.

At Hagley Primary School Primary School, we have planned a curriculum that ensures the following:

- Specific online safety lessons are delivered following a progressive theme across the school from Foundation Stage to Year 6 (following Project evolve and the 8 Areas of Learning: online reputation, cyber bullying, privacy and security, managing online information, self-image and identity, copyright, online relationships and health, well-being and lifestyle.)
- Pupils are taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information.
- Pupils are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils build awareness of and resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.

- Pupils who have achieved lower than expected outcomes in any areas linked to online safety and pupils with language and communication barriers will receive pre-teaching of earlier year group lessons to overcome difficulties in accessing the lesson.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies
- Complete lessons linked to Project Evolve ensuring full coverage of all 8 areas identified within this curriculum (this is not an exhaustive list)

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Complete lessons linked to Project Evolve ensuring full coverage of all 8 areas identified within this curriculum
- Identify a range of ways to report concerns about content and contact (this is not an exhaustive list)

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to
- report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

5. Cyber-bullying

5.1 Definition

Cyberbullying (or online bullying) is bullying using technologies, particularly over the internet or via mobile and gaming networks to deliberately and repeatedly upset someone else. Cyberbullying can be an extension of face-to-face bullying, with technology providing an additional route to harass an individual or group. Cyberbullying can include: intimidation and threats, harassment and stalking, vilification/defamation, exclusion or peer rejection, impersonation, unauthorised publication of personal information or images and manipulation (Taken from Childnet.com).

5.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying

with their classes, and where appropriate the issue will be addressed in assemblies as well as other planned opportunities such as Online Safety Week.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on online safety which includes cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

Hagley Primary School will (when appropriate) also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and relationships policy as well as following relevant guidance from the DfE. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSLs will consider whether the incident should be reported to the police if it involves illegal material, or there is reason to believe that a young person has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent, and will work with external services if it is deemed necessary to do so. This also applies to incidents relating to the sharing of consensual and non-consensual nudes and semi-nudes.

5.3 Examining electronic devices

If it is reported that a pupils has inappropriate material on an electronic device, it will be reported immediately to the DSL/DDSL in line with our safeguarding procedures. The DSL/DDSL will then decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

6. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1-3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1, 2 and 3.

7. Pupils using mobile devices in school (Please also refer to the Mobile Phone Policy)

While we fully acknowledge a parent's right to allow their child to bring a mobile phone to school if they walk to and from school without adult supervision, Hagley Primary School Primary discourages pupils bringing mobile phones in year groups below Year 5 & 6. Phones are turned off and left securely with their class teacher on arrival into the school building. Children are not permitted to use them during the school day or during any extended before and or afterschool activity.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1). Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour and relationships policy, which may result in the confiscation of their device.

8. Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their school device, they must seek advice from the network manager/business manager.

Work devices must be used solely for work activities.

9. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

10. Training

All new staff members will receive training, as part of their induction, on the use of the school network, including cyber- security and online safety including the risk of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, 7-minute briefing updates and staff meetings).

The DSL and DDSL's will undertake child protection and safeguarding training, which will include online safety, annually. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on cyber security and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

11. Monitoring arrangements

This policy will be reviewed every year by the Online Safety Lead and DSLs. At every review, the policy will be shared with the governing body and staff.

12. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour Policy
- Staff Code of Conduct
- GDPR Data Protection Policy including Freedom of Information

- Complaints procedures
- Mobile Phone Policy

Appendix 1

Acceptable use agreement

Please return to Tina Rennie, School Business Manager, ensuring that both forms are completed

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

I understand that when using my personal technology (phone, email etc.) in school that I am still subject to the guidelines set out in the e-safeguarding policy. Any use of personal technology, email or social networks must be safe, reasonable and not interfere with or become detrimental to the role being carried out in school.

I understand that as a member of staff or volunteer at the school, I should share data about the school and its pupils safely, and should represent the school in a positive light.

I understand that personal relationships with parents and carers of pupils could result in a conflict of interest. As a result, I understand that I am expected to remain professional in order to protect the safety and confidence of the pupils and staff of the school.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, learning platform) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school in the online safety policy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, to the appropriate person (Online safety Officer or Headteacher).

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital images. **I will not use my personal equipment to record these images.**
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the Online safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the Online safety policy)

- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the Online safety policy)
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will only use my personal mobile ICT devices as agreed in the Online safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will never use my personal ICT equipment to take or store images of or data about pupils of Hagley Primary School.
- I will not use personal email addresses on the school ICT systems except in an emergency (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (see e-security policy). Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including images, music and videos).

I understand that I am responsible for my actions in and out of school:

I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and to my use of personal equipment in school or in situations related to my employment by the school.

I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see section A.2.6).

I understand if the item is accidentally broken that there may be a cost.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Name:	
Signed:	
Date:	

Note:

Alongside this acceptable use agreement, could you please sign the document below to indicate that you have been given a school laptop and/or Ipad. This will help us to keep track of the technology we have available in school and also quickly return items should there be any technical errors or updates.

Hagley Primary School

Laptop/iPad Agreement

I, …….. am signing for

Hagley Primary School Laptop/iPad number (green sticker):	
Make and model:	
Serial no.:	
Problems concerning equipment:	

The laptop remains the property of Hagley Primary School and I agree to take responsibility for it when taking it off the school site by ensuring that:

- The laptop/iPad is carried safely in the laptop bag provided or in a suitable bag provided by myself.
- I understand our insurance does not cover laptops and iPads left in unattended vehicles.
- I understand that I must have adequate home insurance to cover the laptop/iPad when taking it home.
- I agree to return the laptop/iPad at the end of my contract.
- I agree that there may be a cost involved if the item is broken or damaged and required repair or replacement.

Signed:…….. Date…….