Hallcroft Infant & Nursery School

Online Safety & Mobile Phone Policy November 2026

Agreed by Governors - November 2026

Review Date – Annually as required in KCSIE

Contents

1. Aims

2. Legislation and guidance

3. Roles and responsibilities

4. Educating pupils about online safety

5. Educating parents about online safety

6. Cyber-bullying

7. Acceptable use of the internet in school

8. Pupils using mobile devices in school

9. Staff using work devices outside school

10. How the school will respond to issues of misuse

11. Training

12. Monitoring arrangements

13. Links with other policies

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Appendix 3: online safety training needs – self audit for staff

Appendix 4: online safety incident report log

1. Aims

Our school aims to:

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

→ Deliver an effective and interrelated approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones' but is not exclusive to mobile phones and might include tablets, smart devices such as watches, virtual assistants, gaming machines et al)

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

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content: -** being exposed to illegal, inappropriate, or harmful content, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories,
- **Contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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:** behaviour that increases likelihood of harm for example, making, sending and receiving explicit images, including those generated using AI and online bullying, and
- **Commerce:** risks such as gambling, inappropriate advertising, phishing and financial scams

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 and cyber-bullying: advice for headteachers and school staff

→ Relationships and sex education

→ Searching, screening and confiscation

It also refers to the DfE'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.

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 to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governor who oversees online safety is Phil Metcalfe (Safeguarding Governor)

All governors will:

- → Ensure that they have read and understand this policy
- → Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)
- → Ensure that children be taught about safeguarding, including in relation to online safety and that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable
- → Ensure that all staff undergo 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 – at induction and regularly updated
- → Ensure that children be taught about safeguarding, including in relation to online safety
- → Review the DfE Filtering and Monitoring Standards and discuss with IT staff and service providers what more needs to be done to support the school in meeting this standard

3.2 The headteacher

Senior leaders set the culture and ensure that systems are effective. In line with KCSIE, the DSL holds day-to-day lead responsibility.

Senior leaders will:

- → Ensure the school meets its safeguarding duty of care, including online safety.
- → Know and apply procedures for serious allegations involving staff.
- → Ensure that the DSL/OSL, IT provider/technical staff and relevant colleagues are trained and able to fulfil their roles.

→ Ensure that all staff receive appropriate online safety training which, amongst other things, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring

→ Ensure that children are taught about how to keep themselves and others safe online, recognising that effective education will be tailored to the specific needs and vulnerabilities of individual children.

→ Put in place appropriate oversight and support for internal monitoring activity.

→ Establish and receive regular online safety reports and act on emerging risks and themes.

→ Monitor the reports from the weekly filtering and monitoring alerts from Lightspeed

→ Work with the DSL and IT provider on the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded.

3.3 The designated safeguarding lead

KCSIE (Para 125) states that the DSL leads safeguarding and child protection, including online safety, and understands filtering and monitoring systems and processes. KCSIE requires this to explicit in the DSL's job description.

The DSL will:

→ Lead safeguarding, including online safety, with clear responsibilities in their job description.

→ Maintain up-to-date knowledge of online risks, filtering/monitoring and cyber security.

→ Coordinate and record online safety concerns and incidents, escalating and referring in line with safeguarding procedures.

→ Liaise with the Online Safety Governor, the IT provider and relevant external partners as required.

→ Review anonymised incident patterns and filtering/monitoring information.

→ With the IT provider, lead the (at least annual) review of the effectiveness on filtering and monitoring systems and ensure that these are recorded

→ Report regularly to Governors and drive continuous improvement across relevant policies and practice, using evidence (e.g. incident data, monitoring.)

3.4 The IT Provider / Technical Support

The IT provider (Jasmine IT) supports leaders and the DSL to meet DfE filtering, monitoring and technical standards. Where services are outsourced, the school remains accountable.

The IT provider will:

- Maintain secure infrastructure and managed user access.
- Implement, maintain and update filtering and monitoring; provide reports; act on alerts and concerns.
- Support procurement, risk identification, reviews and checks with SLT/DSL.
- Monitor systems for misuse and report concerns promptly to the Head Teacher.
- Follow the school's Online Safety and Technical Security policies and keep technical knowledge current.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are expected to uphold professional standards online and contribute to a strong safeguarding culture.

Staff will:

- Follow the Online Safety Policy, Safeguarding/Child Protection Policy, Technical Security Policy and sign/comply with the Staff AUA.
- Maintain professional boundaries (including online/remote learning).
- Supervise learner use of technology and follow procedures for online safety issues
- Embed online safety where appropriate; teach research skills, copyright and plagiarism awareness.

- Challenge harmful online behaviour and report concerns promptly.
- Use only school-approved digital services and AI tools; protect data, apply UK GDPR, and verify AI outputs for accuracy/bias before use.
- Complete induction and annual training, with updates as needed; contribute to improvement by sharing learning and concerns.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensure that pupils follow the school's terms on acceptable use (appendix 1)

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are key partners in reinforcing safe online behaviour.

The school will:

- Publish the Online Safety Policy and share the learner AUA.
- Provide guidance on the responsible use of online technologies and seek permissions for digital services/images where required.
- Share updates through meetings, newsletters, online channels and campaigns.

Parents/carers will be encouraged to reinforce key messages and support safe use of personal devices (where permitted in school).

3.7 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. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

4. Educating pupils about online safety

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

The school delivers a planned, progressive and inclusive programme of online safety education for all learners, aligned to nationally recognised guidance and frameworks.

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

The programme develops learners' ability to:

- recognise and manage online risks, including harmful content, contact, conduct and commerce risks;
- understand consent, sexual harassment and sexual violence (including online), supported by safe opportunities for discussion;
- think critically about what they see online, including how to check reliability and accuracy and the role of AI-generated content;
- respect copyright and intellectual property, including when using online material and AI tools;
- understand and follow the learner acceptable use agreement, and act within moral and legal boundaries;
- understand why online services use minimum-age requirements and how these may support safety, privacy and wellbeing
- make informed decisions about participation in social media, messaging, gaming and other online communities, including services they may not yet be permitted to use
- understand that legal or platform restrictions do not remove the need to learn about online relationships, harmful content, image sharing, scams, exploitation and digital wellbeing

- understand the school's mobile-phone requirements and the safeguarding, behaviour, learning and wellbeing reasons that underpin them.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 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.

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

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school 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 policy. 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 DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

Pupils are not allowed to bring any electronic devices into school and any that are brought into school will not be examined and kept securely in the main office.

7. 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 & 2). 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 and 2.

8. Using mobile and smart devices in school

Pupils are not permitted to bring mobile or smart devices into school.

Any mobile or smart devices brought to school by pupils, must be stored in the main office for safe keeping until the end of the day.

Any use of mobile or smart devices in school must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff (including volunteers, contractors and anyone else otherwise engaged by the school) are not permitted to use their personal mobile phone, while children are present. Staff may use mobile or

smart devices during their break times and in an appropriate place such as the staff room or an empty classroom where pupils are not present. At all other times, these should be stored safely either in teacher cupboards or in staff lockers. Smart watches are permitted but should have connections to cameras on mobile phones disabled.

A school mobile phone will be kept in the Head Teacher's office for use in school eg. celebration assemblies. It will be available for staff to take on off-site trips to use for photographs, in this instance staff will connect it to the internet using their personal hotspots in order to allow Facebook posts to be made to update parents.

There may be circumstances in which it's appropriate for a member of staff to have use of their phone during contact time for personal reasons. For instance (this list is non-exhaustive): For emergency contact by their child, or their child's school In the case of acutely ill dependents or family members To monitor blood glucose levels The headteacher will decide on a case-by-basis whether to allow for special arrangements.
Any use of mobile devices in school must be in line with the acceptable use agreement (see appendices 1 and 2).
Any breach of the acceptable use agreement may trigger disciplinary action in line with the staff code of conduct.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- → Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- → Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device

→ Making sure the device locks if left inactive for a period of time

→ Not sharing the device among family or friends

→ Installing anti-virus and anti-spyware software

→ Keeping operating systems up to date – always install the latest updates

→ Storing the device in a safe place, for example not leaving the device in a car overnight.

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

10. 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 ICT and internet acceptable use policies. 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 disciplinary procedures/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.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks 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, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- → Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- → Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- → Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element Training will also help staff:
    - develop better awareness to assist in spotting the signs and symptoms of online abuse
    - develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
    - develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. 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 safe internet use 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.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every year by the DSL and headteacher. At every review, the policy will be shared with the governing body. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with other policies

This online safety policy is linked to our:

→ Child protection and safeguarding policy

→ Relationships and Behaviour policy

→ Staff disciplinary procedures

→ Data protection policy and privacy notices

→ Complaints procedure

→ Computing policy

→ Relationships, Sex and Health Education Policy

→ PHSE Policy

→ Anti-Bullying Policy

→ Child on Child Abuse Policy

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS
Name of pupil:

Appendix 2: Acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS,VOLUNTEERS AND VISITORS
Name of staff member/governor/volunteer/visitor:

Appendix 3: online safety training needs – self audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 4: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**