

Hall Green Primary School



Acceptable use of ICT, Internet & E-mail Policy.

Summary for Pupil & Parental Agreement

Hall Green School's Acceptable Policy

Name of School: Hall Green Primary

Date: May 2026

Review date: May 2027

Introduction

This policy outlines the acceptable use of ICT equipment at our school by staff, volunteers and pupils. It also includes use of access to the internet, use of emails and social media, use of mobile phones, wearables such as glasses or watches with phone or camera capabilities, photography and film permissions as well as data protection whilst using hardware. This policy is available on the school website and parents/carers can ask for a free copy from the school office.

This Acceptable Use Policy is intended to ensure:

- that staff, volunteers and pupils will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of ICT in their everyday work.

All users of school ICT systems will be required to read and agree to an Acceptable Use Agreement. These are tailored to age and understanding and explain the rules pertaining to safe and permitted use of the school resources. (see Appendices)

Internet access in school

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

The purpose of internet access in schools is to raise educational standards, support the professional work of staff and enhance the school's management, information and business administration systems.

Teachers and pupils will have access to web sites worldwide offering educational resources, news and current events.

In addition, staff will have the opportunity to: access educational materials and good curriculum practice; communicate with the advisory and support services, professional associations and colleagues; exchange curriculum and administration data with the LA and DfES; receive up-to date information and participate in government initiatives.

The computer network, iPads and laptops are owned by the school and may be used by children to further their education and by staff to enhance their professional activities including teaching, research, administration and management.

Using the Internet to enhance learning

Access to the Internet is a planned part of the curriculum that enriches and extends learning activities. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use.

Different ways of accessing information from the internet are used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other-adult) demonstration
- Pupils may access teacher-prepared materials, rather than the open internet
- Pupils may be given a suitable web page or a single web site to access
- Pupils may be provided with lists of relevant and suitable web sites which they may access
- Pupils may use teacher-directed search engines to aid their learning, under close supervision and with school filters in place
- Pupils are expected to observe the rules of responsible internet use and are informed that checks can and will be made on files held on the system and the sites they access
- Pupils will be educated in taking responsibility for their own internet access

Using information from the Internet

- Pupils are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium)
- When copying materials from the Web, pupils are taught to observe copyright
- Pupils are made aware that the writer of an e-mail or the author of a web page may not be the person claimed

Ensuring Internet access is appropriate and safe

In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. The school will take every practical

measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- Children are taught safe ways to access information, using child friendly search engines
- Our internet access has a filtering system which prevents access to material inappropriate for children; Senso/SIPS IT must be contacted by the Computing lead or Class teacher if the pupils see any inappropriate sites on line in order for them to be filtered accordingly
- Children using the internet will be working in the classroom or shared area within the school and will be under the supervision of an adult at all times
- Staff will use their professional judgement and check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils
- Our rules for responsible internet use are shared and children are made aware of these and asked to sign an age appropriate Acceptable Use Agreement
- The Computing lead will ensure that occasional checks are made on files to monitor compliance with the school's Acceptable Use Policy
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider and the DfES

A most important element of our rules of responsible internet use is that pupils will be taught to tell a teacher **immediately** if they encounter any material that makes them feel uncomfortable.

If there is an incident in which a pupil is exposed to offensive or upsetting material the school will respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children is taken by the Computing Lead, the Designated Safeguarding Lead and the pupil's class teacher. All teaching staff will be made aware of the incident at a staff meeting if appropriate, or via email.

- If one or more pupils discover (view) inappropriate material, our first priority will be to give them appropriate support. The pupil's parents/carers will be informed and given an explanation of the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue;
- If staff or pupils discover unsuitable sites the Computing subject leader will be informed. They will report the URL (address) and content to the Internet Service Provider (LGfL) and SIPS IT; if it is thought that the material is illegal, after consultation with the ISP and LA, the site will be referred to the police.

Using email

Pupils learn how to use an email application and are taught email conventions. Staff and governors use school email to communicate with others, to request information and to share information. Email addresses are password protected and should not be shared with others. Children must only use school email addresses to communicate with each other as part of the Computing curriculum.

- Pupils are only allowed to use email once they have been taught the rules of responsible internet use and the reasons for these rules.
- Teachers endeavour to ensure that these rules remain uppermost in the children's minds as they monitor children using email.
- Pupils may send email as part of planned lessons but will not be given individual email accounts.
- Incoming email to pupils will not be regarded as private; emails from students should not be responded to unless on a school email account.
- Children will have the email messages they compose checked by a member of staff before sending them.
- The forwarding of chain letters will not be permitted.
- Pupils are not permitted to use email at school to arrange to meet someone outside school hours.

Photography

- Only school cameras, iPads and computers will be used to take photographs of students; photographs must be downloaded at school or onto school equipment.
- Parents/carers will be asked when the children start school and during any administration reviews to give permission for their child to have their photograph taken and used in a variety of contexts: on display in school; on the website; in the local press; on social media; film footage in school; films to share with classmates; film on social media and image in the National press.
- Parents, carers and visitors to school are reminded about not sharing photographs/films during performances on social media and opportunities are given where possible to take photos/films of their own child.

The School Website

Our school website is intended to:

- Provide accurate, up-to-date information about our school.
- Follow the statutory guidance of the DfE.
- Provide pupils with the opportunity to publish their work on the internet for a very wide audience including pupils, parents, staff, governors, members of the local community and others.
- Celebrate successes.

- Provide links to other recommended websites for pupils, parents, staff, governors and supporters.
- Promote the school.

The point of contact on the web site will be the school address, telephone number and email address. We do not publish pupils' full names or photographs that identify individuals on our web pages. Home information or individual email identities will not be published. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our web site.

The website address is: www.hallgreenprimary.co.uk

Social Media Sites

Pupils are taught that they should not have profiles on sites such as Facebook (must be 13 years old to have an account). Staff may have social networking profiles; however, they must not make friends with pupils and report any concerns or contact made from pupils to the Designated Safeguarding Lead. It would also be best practice not to be friends with any parents from the school due to links with the social media community; children would also be able to access information at home through the parent's profile.

- Staff are not permitted to write any derogatory remarks about school on Social Networking sites.

Any concerns should be reported to the Head Teacher to investigate and address.

Passwords

Staff computers should have logins, as well as email accounts. Passwords should not be shared with others. Pupils have logins to school ipads.

- Users should not logon to or use any account other than their own
- Users should always logoff when leaving a workstation/laptop, even for just a short period of time
- Laptops that are taken home with pupil information on should be password protected **and encrypted**

Safer Working Practice

This policy should be used in conjunction with our safeguarding policies.

Mobile Phones and Smart Watches with Phone/Camera Capabilities

Staff have personal mobile phones which will be taken on school trips, residentials and other school events. Communication with parents should take place through a nominated school representative, for example, the school office. Staff should never share their personal phone number or details with a pupil or parents/carers. Staff must

not contact pupils by text or mobile phone and vice versa. No photos or films of pupils should be taken on personal devices including mobile phones and smart watches with phone/camera capabilities.

Teaching staff's mobile phones and smart watches with phone/camera capabilities should not be on view in classrooms. A member of the Senior Management Team should be informed if a member of staff needs their phone to be accessible during learning or school time due to an emergency. Staff are able to use their mobile phones in emergencies to safeguard e.g. making calls to other staff members or emergency services. Generally, staff should limit the use of their mobile phones to their break or lunchtime.

Pupils may be given mobile phones and smart watches with phone/camera capabilities by their parents/carers to safeguard them walking to and from school. Mobile phones and any other devices with phone/camera capabilities should be handed in to the class teacher during the school day to restrict unauthorised use in school. No photos or films should be taken by pupils at school.

Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) technology is already widely used in commercial environments and is gaining greater use in education. We recognise that the technology has many benefits and the potential to enhance outcomes and educational experiences, with the opportunity to support staff in reducing workload.

We also realise that there are risks involved in the use of AI systems, but that these can be mitigated through our existing policies and procedures, amending these as necessary to address AI risks.

We will educate staff and learners about safe and ethical use of AI, preparing them for a future in which AI technologies are likely to play an increasing role.

The safeguarding of staff and learners will, as always, be at the forefront of our policy and practice.

The school acknowledges the benefits of the use of AI in an educational context - including enhancing teaching and learning and outcomes, improving administrative processes, reducing 5 workload and preparing staff and learners for a future in which AI technology will be an integral part. Staff are encouraged to use AI based tools to support their work where appropriate, within the frameworks provided in the Artificial Intelligence in Schools policy and are required to be professionally responsible and accountable for this area of their work.

Staff must prioritise human oversight. AI should assist, not replace, human decision-making. Staff must ensure that final judgments, particularly those affecting people, are made by humans and critically evaluate AI-generated outputs. They must ensure that all AI-generated content is fact checked and reviewed for accuracy before sharing or

publishing. This is especially important for external communication to avoid spreading misinformation.

Staff must not use AI tools with children in the classroom, unless agreed with SLT, such as AIR and must ensure that no school sensitive data or personal information is uploaded to AI Tools, unless permission is granted.

Other policies

This policy will be used in conjunction with these policies:

- Acceptable User Agreements
- Anti-Bullying Policy
- Artificial Intelligence in Schools Policy
- Attendance
- Complaints
- Child Protection/Safeguarding Policy
- E-Safety Policy
- First Aid and Medication
- Health and Safety
- Keeping Children Safe in Education – Part 1 (most up to date version)
- Offsite Visits
- SEND Local Offer
- Safeguarding
- Safer Recruitment and staff HR policies
- Safer Working Practice
- Special Educational Needs and Disabilities (SEND)
- Staff Behaviour - Code of Conduct and Teaching Standards
- Whistle Blowing
- Working Together to Keep Children Safe

This policy was written in May 2026

Ratified by the Governors: _____ Date: _____