Hindley J and I School

Acceptable Use of ICT Policy

Updated: February 2025

Signed on behalf of the School: Miss A Mckeever

Signed on behalf of the Governors: Mr G Doubleday

The implementation of this policy is the responsibility of all members of staff

Introduction

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff and governors. It supports teaching and learning, pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Support the school's policy on data protection, online safety and safeguarding
- Prevent disruption to the school through the misuse, or attempted misuse, of ICT systems
- Support the school in teaching pupils safe and effective internet and ICT use.

This acceptable use agreement is designed to outline users 'responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises.

This Agreement intends to ensure:

- That users will be responsible and stay safe whilst using the internet and other technologies for educational, personal and recreational use *(Any misuse of technology will not be taken lightly and will be reported to the Headteacher in order for any necessary further action to be taken.)*
- 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 and personal lives.

This policy covers all users of our school's ICT facilities, including governors, staff and pupils.

Users are asked to read 'their' document carefully, and sign to show they agree to the terms outlined. Please see below for the different Acceptable Use Agreement Forms within this policy:

- Appendix 1: Acceptable Use Agreement Form for pupils
- Appendix 2: Acceptable Use Agreement Form for Staff, Volunteer and Community Users

Roles and responsibilities

The governing board

- The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

- The governing board will also make sure all staff receive regular online safety updates, as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
- The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
- The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness.

The headteacher

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

The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT technician to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT technician and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

The ICT technician / Headteacher/Business Manager

The ICT technician / Headteacher/Business Manager are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept 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
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Use physical monitoring whilst the children are using IT systems/laptops.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting it to SLT/Office staff.
- Following the correct procedures by reporting it to SLT/Office staff/technician if they need to bypass the filtering and monitoring systems for educational purposes
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

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).

Educating pupils about online safety

Hindley Junior & Infant School will ensure that adults and children will have access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect all adults and children to agree to be responsible users. We understand that the internet is a valuable resource that can raise educational standards by offering pupils and teachers opportunities to search for information from a very wide range of sources based throughout the world. However, there are significant risks to using the internet which this policy intends to mitigate.

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- PSHE
- Computing

The curriculum and the school's approach to online safety is developed in line with the DfE's 'Teaching online safety in school' guidance. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

Online safety teaching is always appropriate to pupils' ages and developmental stages.
The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online

- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Supervision of Pupil Use when using ICT Equipment

The school operates sophisticated classroom monitoring solutions to help staff with the supervision of students when using computer equipment.

Pupils must be supervised at all times when using computer equipment.

Staff are responsible enforcing the pupil Acceptable use policy when using computer equipment.

The internet in School

The internet is a powerful technology, and we realise that it plays an important role in any learning environment. Through the internet, teachers are able to find information on topics they may be teaching. It aids planning and collaboration between schools. It also provides an e-mail address to members of staff to enable them to keep in contact with colleagues, parents and other schools.

The Internet in the Curriculum

The use of the Internet in the curriculum needs careful planning, and it should not be assumed that the children have the skills and knowledge of how to work safely in an online environment – for example, how to use search engines safely. Therefore, if the internet is to be used, the teacher should ensure that these points are covered in the interests of accessibility, and also of safety.

Managing the School Network

The computer system/network is owned by the school and is made available to pupils to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

The school reserves the right to examine or delete any files that may be held on its computer system to monitor any internet or email activity on the network or perform any other activities that the school may see fit, in accordance with data protection and GDPR legislation.

Use of AI

The school recognises that there can be many benefits regarding the use of AI to support and enhance teaching and learning. This however should be used with caution and good awareness of the risks that it can present to ensure this can be used both safely and effectively.

Personal use

Hindley J and I School recognises that mobile technology offers valuable benefits to staff from a teaching and learning perspective. This policy is intended to address the use by staff members on non-school owned electronic devices to access the internet via the school's internet connection or to access or store school information. These devices include smart phones, tablets, laptops, wearable technology and any similar devices. These devices are referred to as mobile devices in this policy.

Staff must only use mobile devices in the staff room or in an office during free time, unless as part of a planned lesson or access is required e.g. authentication app.

Access to the School's internet connection

The school provides a wireless network that staff may use to connect their mobile devices to the internet. Access to the wireless network is at the discretion of the school and the school may withdraw access from anyone it considers is using the network inappropriately.

The school cannot guarantee that the wireless network is secure and staff use it at their own risk. In particular staff are advised not to use the wireless network for online banking or shopping.

The school is not responsible for the content of any apps, updates or other software that may be downloaded onto the user's own device whilst using the school's wireless network. This activity is taken at the owner's own risk and is discouraged by the school. The school will have no liability whatsoever for any loss of data or damage to the owner's device resulting from use of the school's wireless network.

Access to school IT Services

School staff are permitted to connect to or access the following school IT services from their mobile devices however their mobile device **MUST HAVE** the latest software on it, all apps **MUST** be updated as and when required and **MUST HAVE** SOPHOS protection or similar on:

- The school email system
- One Drive
- Class Dojo
- Authentication app
- CPOMS
- Arbor MIS
- Insight
- Inventry.

Staff may use the systems listed above to view school information via their mobile devices, including information about pupils. Staff must not store the information on their devices, or

on cloud servers linked to their mobile devices. In some cases it may be necessary for staff to download school information to their mobile device in order to view it (for example to view an email attachment). Staff must delete this information from their devices as soon as they have finished viewing it. Where personal or sensitive data is used in this way devices or files **MUST** be encrypted.

School information accessed through these services is confidential, in particular information about pupils. Staff must take all reasonable measures to prevent unauthorised access to it. Staff must not send school information to their personal email accounts.

Staff must take all reasonable measures to prevent unauthorised access to their mobile devices including, but not limited to the use of a PIN, pattern or password to be entered to unlock the device and ensuring that the device auto-locks if inactive for a period of time.

Staff **MUST** ensure that appropriate security software is installed on their mobile devices and must keep the software and security settings up to date.

Non-compliance of this policy exposes both staff and the school to risks. If a breach of this policy occurs the school may discipline staff in line with the school's Disciplinary procedure. Guidance will also be offered to staff to support them in complying with this policy. If steps are not taken by the individual to rectify the situation and adhere to the policy, then the mobile device in question may be confiscated and/or permission to use the device on school premises will be temporarily withdrawn. For persistent breach of this policy, the school will permanently withdraw the permissions for staff to use user-owned devices in school.

The school takes any security incident involving a staff member's personal device very seriously and will always investigate a reported incident. Loss of theft of a mobile device should be reported to the School Business Manager and Headteacher.

Passwords

To protect our school data, our school network and our mobile devices, staff need to ensure they adhere to the following principles when setting passwords.

- Have a different password for each account/service you use
- If you must write down your passwords store them securely and away from your device
- Use two factor authentication (2FA) when accessing services in school which hold sensitive information e.g. CPOMS, Class Dojo, Insight, School emails, Arbor MIS
- Use four random words, numbers and special characters
- DO NOT USE names, the word password, qwerty, pet's names etc.
- Change your passwords on a regular basis (at least every term).

Use of removable Storage Devices

USB memory sticks and other removable storage devices have become increasingly popular because of their small form appearance and large storage capacity. This has made them very convenient devices for carrying files from one place to another. However, this way of storing data has introduced new security risks:

- Loss of information – a memory stick, like a computer, is susceptible to data loss or failure.
- Potential breach of data confidentiality – if the memory stick is lost or stolen.
- Loss of physical device – being so physically small the memory stick can be easily lost.
- Corruption of data - if the memory stick is not removed from a computer properly.
- Malicious content transmission – memory sticks can introduce viruses onto our internal computer network.

As such, the school have taken the decision to prohibit the use of any storage devices on the internal school network. Instead, Microsoft OneDrive for Business has been issued to all staff for data storage. This eliminates the security risks identified above.

Appendix 1

Acceptable use Agreement Form for Pupils at Hindley Junior and Infant School

As a pupil at Hindley Junior and Infant Primary School, I understand that the school has installed computers and Internet access to help my learning.

These rules will keep myself and everyone else safe.

• I will keep my personal information safe and not share it with people online.

• I will only use the software and websites that my teacher has asked me to use.

• I will keep my passwords safe from other people.

• I will not copy another pupil's work and say that it is my own.

• I will let an adult know straightaway if I accidentally see something inappropriate.

• I will respect the hardware and equipment.

• I will be responsible for my behaviour online and will be kind to others.

• I will only access my own files.

• I will not change any settings on the computers without permission from my teacher.

• I will not download any apps onto the i-pads or computers without permission from my teacher.

I understand that if these rules are not followed, I may be issued with a consequence.

Pupil Signature: _____

Year Group: _____

Date: _____

Appendix 2

Acceptable Use Agreement Form for All Staff

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning, and I will ensure that children receive opportunities to gain from the use of digital technology. I will, where possible, educate the children in my care in the safe use of digital technology and embed online safety in my work with children.

Please tick to agree ☐

I understand that this Acceptable Use Policy 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 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 Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and/or the Local Authority and in the event of illegal activities the involvement of the police.

Please tick to agree ☐

I will only use strong passwords using the guidance provided in this policy and will change my passwords on a regular basis.

Please tick to agree ☐

I will no longer use any USB devices to store any school data and will not use these on any device belonging to school or used on the school network/internet.

Please tick to agree ☐

I will ensure my own personal device is kept up to date with the latest security/software updates and will not access any school data or services if this is no longer the case

Please tick to agree ☐

Whilst using my mobile device, I will use two factor authentication (2FA),where available, to access any systems with sensitive data e.g. CPOMS, Class Dojo, Evolve, Arbor MIS, Insight etc.

Please tick to agree ☐

Name: _____ ***Signed:*** _____

Date: _____