



Challenge, Equality & Opportunity

Acceptable Use and Online Safety Policy 2024

Scope

This policy applies to:

- All staff users of the school network including all information systems accessed through it; this includes but is not limited to employees, contractors, consultants, external auditors, trainee teachers and temporary/casual staff, including those from private Supply Agencies.
- All children who use the school network, including access to the internet and online resources.
- All other users of the school network, for example visitors who are granted access.
- All the school's information whether held on paper or electronically, and computing equipment, including (but not limited to) computers, servers, iPads, printers, telephones, cameras and hand-held devices such as tablets and smart phones.
- All school owned computing assets including but not limited to laptops, desk tops, iPads and mobile devices.
- All the school's data and all reports derived from such data.
- All programs developed by school employees or on behalf of the school, using school equipment or personal computers used for home working by school employees.
- All communication lines, and all associated equipment or devices used on school premises or connected to school resources that are capable of processing or storing the school's information; this includes all electronic devices used in school whether belonging to the school or personal devices owned by individuals.

Aims

The aims of this policy are to ensure that:

- We have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- We deliver an effective 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.
- All information and information systems on which the school depends are adequately protected to the appropriate level. This includes the IT infrastructure for the retrieval, sharing and dissemination of business critical data and conducting daily transactions.

- All staff and other users are aware of their responsibilities for processing personal information under the Data Protection Act 2018.
- All adult users are aware of their accountability and that they are aware the failure to comply with the Information Security Policy is possibly a civil or criminal offence.
- Information assets, computers and communication systems that are owned by the school and supported by IT Services are protected against external and internal threats.

Havannah First School can receive support in implementing this policy from IT Services at the Local Authority, GEM Education and HR Services at the Local Authority; these services are committed to supporting the protection of the security of the school through the preservation of:

Confidentiality – protecting information from unauthorised access and disclosure.

Integrity – safeguarding the accuracy and completeness of information and processing methods.

Availability – ensuring that information and associated services are only available to authorised users when required.

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 access to the internet and digital technologies at all times.

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.
- Education for a connected world.
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff.
- 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 2011, 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.

Relationship with other policies and procedures

Please also refer to:

- Code of conduct: this sets out the standards expected of staff
- Disciplinary procedure: schools must follow their disciplinary procedure where it is appropriate to take such action against an employee.
- Whistle-blowing policy
- Behaviour Policy (for children in school)
- Safeguarding policy
- Data Protection Act policy/Fair processing notice
- Teacher iPad policy

ROLES AND RESPONSIBILITIES

All staff should make themselves aware of the contents of this policy and follow it.

The Governing Body has overall responsibility to ensure that the procedure is properly and fairly applied.

The Headteacher is responsible for ensuring that all staff are aware of this policy and comply with the guidance.

Working under the direction of the Headteacher, the **Computing Subject Leader** will be involved in making staff aware of this policy and supporting them in complying with the guidance.

The Online Safety Committee, comprising a member of the Governing Body, the Curriculum Leader and the Headteacher, will monitor the implementation of this policy and review its effectiveness annually.

The experiences and requirements of the various user groups are different, so this policy is divided into three sections. Part A refers to staff users, Part B refers to children at the school, and Part C refers to governors, parents and other visitors.

FIREWALL PROTECTION

The following protection is in place on all school technology to protect information and information systems:

Smoothwall Firewall: - Internet browsing protection and prevention.

Online protection which includes Anti-malware protection, HTTPS inspection, anonymous proxy detection and blocking, and intrusion detection and prevention.

Cisco Firepower Threat Defence Next Generation Firewall.

This secures the perimeter and internal networks, providing access control as well as malware and intrusion scanning and protection.

Part A – Staff uses of School Network and IT Equipment

Staff members represent a key component in the delivery of information security and a secure environment. Investment in secure technology and secure processes is meaningless unless all staff are aware of the role they need to play in security and what is acceptable. Online safety is a whole school issue. The following section outlines areas of personal responsibility for staff members and is intended to provide clear guidance as to the expected role of school staff in providing and maintaining a secure IT/Computing environment in the school. IT Support from the LA and GEM Education are available to work with the school and individual staff members to provide any clarification, training or support required to ensure that everyone understands their roles and responsibilities.

A1.1 Online Safety Awareness and Training

In order to ensure that staff members fulfil their responsibility for IT and Information Security it is essential that appropriate training is provided to ensure an awareness of the legal and procedural expectations placed upon them. To this end, the school will provide training to all existing staff and to all new members of staff in the form of induction training. A 'refresher' session will be held annually.

This training will cover the following key areas:

- Known threats, risks and implications
- Acceptable Use
- Password Guidance

- All staff members will be trained and made aware of their personal responsibility for maintaining information security and their roles in the classification process.
- Awareness of this document and any other relevant school policy documents.

A1.2 Acceptable Use

This section is intended to provide staff members with guidance on acceptable and unacceptable use when using information and the computing facilities provided by school and supported IT services. If there are any questions or concerns, advice can be sought from the Local Authority and other school advisors. The school's Senior Leadership Team may be contacted in the first instance if appropriate.

A1.3 Investigations

If there are any concerns that the policies or guidance within this document have been breached, or there is a suspicion of criminal activity then this must be reported directly to a member of the school's Senior Leadership Team. They will then communicate directly with the Senior Management of IT Services at the Local Authority and Human Resources to discuss any investigation that may be required. Further specialist advice may be sought from other relevant services within the Local Authority, eg the LADO. Breaches of this policy may also result in disciplinary, civil or criminal action. Staff should be aware that school is legally obliged to report any illegal activity which takes place on the school premises or using school equipment to the Police.

A1.4 Using Computing Equipment

Each user is responsible for the equipment that they use, the data it holds and the output produced. This also applies to portable equipment, media or data that is used away from the normal place of work.

Staff – MUST
▪ Keep any portable equipment securely, and carry it safely.
▪ Keep log on details for resources such as Office 365 and RDS safe at all times and report their loss immediately.
▪ Unless instructed otherwise, log off from the network every night and fully shut down the PC/Laptop.
▪ Lock laptop screens when you leave the room, even if you will only be away from the room for a short period of time.
▪ Connect laptops to the network as often as possible to keep the anti-virus and patching protection up to date.
▪ Report any problems as soon as possible to IT Services (via ictservicesdesk@newcastle.gov.uk and to the Computing Subject Leader or a member of office staff) including the loss of, or damage to, any computing equipment.
▪ Ensure that any redundant computing equipment is disposed of in a secure and legal manner; the Computing Subject Leader, working with office staff, will organise this process as the equipment needs to be disposed of appropriately and removed from the school's equipment list. IT Services will provide support in this process.
▪ Ensure that all software used is correctly licensed and covered by a school or Local Authority license (i.e. not home or personal user). The licence terms for free software must be carefully examined to ensure it meets these requirements.
▪ Ensure all software is installed by IT Services (Local Authority).
▪ Only take photographs that are for school purposes using school equipment.
▪ Only save photographs of children on the school network and not on any portable device, including USB memory sticks and laptops; photos taken on the iPads should be transferred to the school network as soon as feasible and deleted from the iPad.
▪ Ensure there are no photos on iPads or any other portable device before removing it from the school building (e.g. for teachers to work off site or for use on a school visit).
▪ Ensure permission has been given by parents before using photographs of children on the school website. (Check permissions saved on the school network.)

Staff - MUST NOT
▪ Allow students or any other member of staff or visitor, to use a machine logged on using your or another person's username and password, except when closely supervised e.g. children using the Smartboard with a teacher's laptop attached in a lesson.
▪ Save any information on to any computer or device which is not registered as school equipment.

- Use personal cameras including mobile phones to take photographs of children from school without prior consent from the Headteacher. In this instance, staff must delete photographs from devices (from camera roll and 'recently deleted') in the presence of a witness from the SLT, on the same day and before leaving the building.
- Take photographs of children from school out of school, except with prior permission from the Headteacher. (E.g. this may be allowed on trips).

Staff – SHOULD

- Lock your PC/Laptop screen (using Ctrl/Alt/Del then 'Lock Computer') whenever you are away from your desk, to prevent someone accidentally or deliberately looking at information, making unauthorised changes, or sending emails in your name.
- Shut down or logout if you are going to be away from your machine for any length of time.
- Report any instances of possible security breaches, including near misses. For example, if:
 - A colleague is using someone else's log-in name and password.
 - You can see personal information on a computer screen in an unattended area.

A1.5 Passwords

Effective username and password combinations are a basic security requirement for any information system. But they are only effective if used properly.

Staff – MUST

Choose a password that:

- Is at least 8 characters long
- Contains at least one letter and at least one numeric character
- Contains both uppercase and lowercase letters and at least one punctuation mark or other 'special character'
- Where the system cannot meet these requirements you will use the maximum complexity that the system allows
- Change your password at least every 90 days (PCs/Laptops will prompt this).
- Change your password as soon as possible, if anyone else gets it know it.

Staff - MUST NOT

- Disclose your password to anyone else.
- Use another person's logon name or password or allow someone to use another person's logon name and password.
- Use another person's machine whilst they are not there if they have not locked it (log the machine off or lock it for them).
- Use the same password twice.
- Write your password down and keep it where anyone else may be able to read or use it.
- Reply to any email asking for your username, log in details or password (even with a refusal since this lets the sender know that they have located a valid email address).

A1.6 Saving Files

Staff – MUST

- Save files on the server rather than on to your PC (including laptops).
- Save files to appropriate locations on the network, taking into consideration the access provided to each drive e.g. the Common drive can be accessed by all users.
- Use Office 365 to access files from the school network at home or elsewhere.
- Restrict access to strictly confidential information on a need to know basis. Help and support is available through the Managed Service to support this process.
- Password protect any documents including confidential information e.g. SEN Reports.

Staff - MUST NOT

- Keep any information on a device in an area where it is particularly vulnerable to theft e.g. Desktop folders.

A1. 7 Using the Internet and Email facilities

All network users have access to the Internet and e-mail. By accepting your network account password and related information, and accessing the network, you agree to keep this policy. You also agree to report any network misuse to the IT Services, the Computing Lead and the School's Senior Leadership Team. Misuse includes policy violations that harm another person or an individual's property.

The school provides each member of staff with an email address. This email account should be used for work purposes only. Staff must enable multi-factor Microsoft authentication on their email account(s). All work-related business should be conducted using the email address the school has provided.

This email account should be used for **work purposes only**. Staff must enable multi-factor Microsoft authentication on their email account(s). All work-related business should be conducted using the email address the school has provided. Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Staff must not share their personal email addresses with parents/carers and pupils, and must not send any work-related materials using their personal email account. Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information. If staff send an email in error that contains the personal information of another person, they must inform the Computing subject lead and office staff immediately and follow our data breach procedure.

A1.8 Mobile Devices including iPads and Laptops

Mobile devices include iPads, laptops and memory sticks and cards, but this list is not exhaustive. Laptops and iPads allocated to teachers are the only type of mobile devices which should be taken off the school premises. In doing so, you must adhere to this policy. 'One Drive' (part of Office 365) should be used to access files from the school network rather than saving them on mobile devices. In exceptional circumstances, a memory stick may be used with the approval of the Headteacher, but staff members are responsible for ensuring sensitive data, for example personal information, is **NEVER** saved on **ANY** portable device. Sensitive data includes children's names, dates of birth, addresses and IEPs, but there are many other examples of sensitive data in school, if you are unsure you should talk to the Headteacher or the Computing Subject Leader. Specific advice and guidance relating to the use of staff iPads can be found in the Teacher iPad policy.

A1.9 Taking and Using Photographs and Videos of Children

When children join Havannah First School, parents/carers will be asked to sign an internet permissions form (See Appendix two). This covers access to the internet, publishing photographs, videos and work. This form covers permission until they leave school at the end of Year 4. Parents/carers sign this form to give permission and are aware that to change permission at any time they must inform the school office.

It is the responsibility of all staff to access and check this information whenever they are publishing photographs of children or their work to the internet or to the media/press.

Taking photographs and videos in school is an important source of evidence of achievement and attainment, and also helps share learning and school events with others e.g. by using them on the website, Twitter and displaying them in school. Guidance on taking photographs and videos is included in this policy for the protection of the children and staff in school.

- Photos and videos taken in school should be taken with a clear purpose in mind, e.g. recording an activity and achievement, and taken at an appropriate, legitimate time.
- They should only ever show the children in a positive light and be appropriate in terms of children's dress, position and behaviour.
- Photos and videos should be saved onto the school network and deleted from the camera as soon as possible.
- Digital or printed versions of the photos and digital videos should not be taken out of school except in exceptional circumstances and with the approval of the Headteacher.

Only school devices should be used to take photographs of pupils. There might be exceptions to this such as taking photographs on visits to use on the school's Twitter account, in these cases prior permission must be sought from the Headteacher. In this instance, once permission has been sought, staff must delete photographs from devices (from camera roll and 'recently deleted') in the presence of a witness from the SLT, on the same day and before leaving the building.

If a member of staff is concerned about the taking and/or use of photographs and videos of children in school, they MUST report this to a member of the school's Senior Leadership Team in order to fulfil their professional responsibilities to the children in their care. If the concern is about a member of the SLT, in particular the Headteacher, staff should report to the chair of Governors. All staff are aware of the whistleblowing policy and what to do with concerns which are considered low level and more serious.

Photographs and videos will be used on the school website (www.havannah.newcastle.sch.uk) and school and class Twitter/X accounts if parental permission has been given. Photographs may also be used in displays around school and newsletters. Photographs and videos on the website and Twitter will not be labelled with the name of the children, and photographs and videos of the children will not be used if their name is in the accompanying text. The press sometimes publish names with photographs, despite school's policy, and this is accounted for in the permission form. Photographs and videos will also be uploaded to the Seesaw app where they can be added to individual child accounts. Tapestry will be used in Early Years to record observations which will include photographs and names of the children. Parents/Carers sign a permission form for the use of Tapestry. The accounts on Seesaw and Tapestry, will be archived each year and monitored by the computing lead.

A.10 Personal Responsibility

- Access to the Internet and email during work hours shall be through a school device attached to the network.
- E-mail access is also permitted via the webmail portal or an authorised mobile device.
- Staff should only use approved e-mail systems within school, such as the schools exchange email to send e-mails related to school business.
- Work related information must not be communicated on non-school e-mail systems. The security of data cannot be guaranteed.
- If other staff need to access your email account (for example, during leave or sickness) you should seek help and support on this area is available through IT Services.
- No information should be sent via email which is prohibited by the Information Asset Policy of Newcastle City Council. Most school information including children's records fall into the 'Protect' category and if these need to be sent electronically, they need to be encrypted. Should this be required, advice should be sought from IT Services. Information about 'Looked After Children' is 'Restricted' and encrypted email must also be used for this.

A1.11 Personal Information

The term 'Personal information' is used frequently in e-safety training and throughout this policy. The term refers to any information that in combination identifies one person to another. This could be a name, address, National Insurance or telephone number. It could also be the type of job they do or the name and location of the school they attend.

- You should take care when sending personal information electronically, this includes uploading or sending information to an Internet site.

A1.12 The security of external communications cannot be guaranteed

Where you have an authorised business need to electronically send sensitive or confidential personal information, which relates to pupils, clients or staff, you must refer to the Information Asset Classification Policy from Newcastle LA. If in doubt, please consult the Headteacher or IT Services.

A1.13 Access to Office 365 including One Drive

Access to files from the school network from locations outside school is granted to teaching staff through use of One Drive, part of the Microsoft Office 365 suite. By uploading files prior to leaving the building, staff are able to access the files when away from school. This is a secure means by which this can occur, significantly more secure than using a laptop's hard drive, a memory stick or an external hard drive which are vulnerable to loss and theft. It also allows access to e-mail away from school.

- Staff members who make use of Office 365 from school should operate to the same acceptable use standards as if they were in school. This includes NOT having personal information including photographs of children stored in this environment. Newcastle LA have assured the school of the high level of security associated with Office 365 (see Subject Leader for further details if required) but files can be downloaded onto other devices and therefore school requires staff not to use Office 365 in this manner.
- You are personally responsible for keeping any work related data stored on any mobile equipment or on Office 365 safe and secure in accordance with the Information Asset Classification Policy from Newcastle LA.

A1.14 Unacceptable Use

Any use of the internet or IT facilities which is against any relevant legislation or any internal school policies is unacceptable and could lead to disciplinary action. If you are in any doubt about any use, you should contact the school's Senior Leadership Team or IT Services.

Examples of unacceptable use include :

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data

- Gaining, or attempting to gain, access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Using 'chat rooms' and 'discussion forums' of a personal, malicious or illegal nature.
- Circulating jokes, personal photographs or making malicious comments about other people on 'social networking sites'.
- Any form of online harassment (or cyberbullying), including harassment by volume of communications on 'chat rooms', 'discussion forums' or 'social networking sites', or sending 'spam'.
- Creating material containing false claims of a deceptive nature.
- Use for private business purposes.
- Any form of gambling.
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way

(This list is not exhaustive.)

Deliberate unlawful or inappropriate material must not be viewed, stored or distributed using the school's IT system or personal devices in school. This can include any material which is in violation of any law or regulation which can be considered by any reasonable person in its context to:

- Be defamatory
 - Be violent
 - Be offensive
 - Be abusive
 - Be indecent or obscene
 - Incite hatred
 - Constitute bullying or harassment
 - Breach anyone's confidence, privacy, trade secrets or copyright.
- Where possible, IT Services will prevent access to material known to be of an offensive or undesirable nature using security tools and filtering software.
 - If you receive an email or access a website which you consider to be offensive or potentially illegal, you must report the matter to the Headteacher, Computing Subject Leader or IT Services.
 - If you receive an email that you consider to be spam, you should forward it to ictservicesdesk@newcastle.gov.uk and then future incoming e-mails from that address can be blocked.

A1.15 Personal Devices including mobile phones

Staff members may use personal devices e.g. Smartphones on school premises, provided they are used outside of working time, not in the sight or presence of children, and not used with children from the school. Personal devices can be connected to the school guest Wi-Fi network which is monitored by the Local Authority and IT Services. Personal devices are for personal use only and all use of personal devices must comply to this policy when used in school. **When on the school site and using your own mobile phone you must comply to all aspects of Acceptable Use as stated in this policy.**

Mobile phones should not be used as part of classroom practice. They should be stored out of sight of children, e.g. in a bag or drawer; they SHOULD NOT be kept on a teacher's desk whilst children are in the classroom. Staff are not allowed to use their mobile phone to take photographs or videos of children in

school for any purpose, other than in exceptional circumstances or with prior permission from the Headteacher.

A1.16 Social Networking

Staff members may use Social Networking sites such as Facebook and Twitter/X for either personal or professional reasons. Forming a Personal Learning Network via social networking sites can lead to significant benefits for their Continuing Professional Development. However, when using sites such as Twitter and Facebook, staff members MUST be aware of the language they use and the comments they make. Privacy settings are not infallible and care should be taken by members of staff to protect their professionalism. The potential audience (e.g. children at the school and their parents, employers etc.) must be considered. It is recommended that comments are not made that would not normally be shared publicly with these groups.

Staff members should not allow access to their own personal areas or open lines of communication with students via social networking sites. It is very important that staff members maintain professional relationships with students at any time and this would be compromised by allowing students access to personal information or photographs.

Use of Social Networking sites for school business (e.g. sharing information with parents, promoting the school etc.) must be through use of a school account e.g. a class account on Twitter.

A2 Monitoring

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school reserves the right to filter and monitor the use of its ICT facilities and network. IT Services will, if requested, facilitate the monitoring of Internet and E-mail facilities and their usage, on behalf of the school to highlight non-compliance. This monitoring will include, but will not be limited to:

- All internet sites staff browse on or through the school network
- All transactions staff make via the internet on the school network
- All files downloaded or uploaded to or from the internet on the school network
- All e-mails sent and received
- All attachments sent and received

Therefore staff should not expect privacy on any e-mails that are sent or received, or websites visited.

Logs are retained on all emails that are sent and received as well as all websites that have been browsed by any user. IT Services may be required to disclose any information kept on computer systems to outside parties or law enforcement authorities. This would always happen in consultation with the school's Senior Leadership Team.

A3 Sanctions

Failure to comply with any of the requirements of this policy may result in further action being taken by the school/local authority in line with the appropriate disciplinary policy. Instances of non-compliance with this policy shall be identified, documented and escalated. Remedial measures shall be implemented by IT Services and school's Senior Leadership Team as quickly as possible. Deliberate non-compliance by individuals, whether they are system administrators or other users, shall be treated as a disciplinary offence, and may also result in civil or criminal action being taken.

Violations of established security procedures and inadvertent and deliberate compromise of School proprietary and personal information are actions that are adverse to the security of a school and as such may warrant disciplinary, civil or criminal action, based on the severity of the incident.

Some breaches of this policy may result in loss of data such as personal information, and this must be reported to the Information Commissioner's Office. The loss is publicly declared and the loss of equipment and/or data must be explained, with the school being held responsible.

Part B – Children using the school network and IT equipment

B1 Guidance

This part of the policy outlines the school's purpose in providing an IT network (including internet access and email facilities) for children at Havannah First School. It also explains how the school seeks to avoid the potential problems that unrestricted Internet access could give rise to. The policy applies to all children who are pupils at Havannah First School, but also applies to members of staff when using the internet with the children.

B2 Internet Access in School

Providing access to the Internet in school raises educational standards and enhances learning opportunities. Children have the right to enjoy childhood online, to access safe online spaces, and to benefit from all the opportunities that a connected world can bring to them, appropriate to their age and stage (Education for a Connected World 2020). All PCs, laptops, netbooks and iPads in school have internet access and children will use the internet to complete tasks related to their work in a range of curriculum areas. It is the responsibility of staff to check the internet permissions for their class prior to allowing children to access the internet in school. Laptops and iPads are available to children only under the supervision of staff. This includes the use of specialist ICT equipment, such as that used for music or design and technology.

B3 Ensuring Internet Access is safe and appropriate – Online Safety

The internet, as a communications medium, is available to any person wishing to send e-mail or publish a web site. In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. Pupils in school are unlikely to see inappropriate content in books due to selection by teachers, and 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:

- Our internet access provides a service designed for children including a "firewall" filtering system intended to prevent access to material inappropriate for them;
- Children using the internet will be working in the classroom or other learning environment, during lesson time and will be supervised by an adult (usually the class teacher) at all times;
- Staff will check that the sites pre-selected for use by the children are appropriate to the age and maturity of pupils;
- Staff will be particularly vigilant when children are undertaking their own search and will check that they are following the agreed search plan;
- Children will be taught to use 'the internet' in all its forms responsibly in order to reduce the risk to themselves and others;
- Our school rules for 'Responsible Use of the laptops and iPads' will be posted in every classroom, taught to children at the beginning of the school year, and then revisited at appropriate points throughout the year;
- Teachers are able to use software such as Apple Classrooms when using school iPads, to quickly and effectively monitor searches and apps that children are using.
- The Computing Subject Leader will monitor the effectiveness of internet access strategies;
- The Computing Subject Leader will ensure that occasional checks are made on files to monitor compliance with the school's Internet Use Policy;
- The Headteacher will ensure that this aspect of the policy is implemented effectively;

- Methods to quantify and minimise the risk of children being exposed to inappropriate material will be reviewed when developments occur and advice from the Local Authority, our Internet Service Provider and the DFE will be sought.
- It is the experience here and in other schools that the above measures have been highly effective. However, due to the international scale and linked nature of information available via the internet, it is not possible to guarantee that particular types of material will never appear on a computer screen. ***Neither the school nor Newcastle LA can accept liability for the material accessed, or any consequences thereof.***

In the unlikely event that an incident in which a child is exposed to offensive or upsetting material occurs, the school will wish to respond to the situation quickly and on a number of levels. Responsibility for handling incidents involving children will be taken by the Computing Subject Leader and in consultation with the Head Teacher and the child's class teacher. All teaching staff and the Online Safety Committee will be made aware of the incident if appropriate.

In the unlikely event that one or more pupils discover (view) inappropriate material, the first priority will be to give them appropriate support. The children'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 children to resolve any issue. If staff or children discover unsuitable sites the Computing Subject Leader will be informed and the incident will be logged. The Computing Subject Leader will report the URL (address) and content to IT Services and seek advice from them; if it is thought that the material is illegal, after consultation with IT Services, the site will be referred to the Police.

The children are expected to play their part in reducing the risk of viewing inappropriate material by obeying the rules for 'Responsible Use of the laptops and iPads', which have been designed to help protect them from exposure to internet sites carrying offensive material.

The DSL, Headteacher or Computing Lead logs behaviour and safeguarding issues related to online safety on CPOMS.

B4 Using the internet as part of the school curriculum

Pupils will learn how to use a web browser and suitable web search engines so they can access the internet to find and evaluate information. Access to the internet will be a planned part of the Computing curriculum that will enrich and extend learning activities and will be integrated into long-term and short-term planning. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use. When accessing the internet on iPads, children will only be able to access through the smoothwall app. This ensures that appropriate filtering and monitoring systems are in place. Different ways of accessing information from the internet will be used depending upon the nature of the material being accessed:

- access to the internet may be by teacher demonstration;
- children may be given a suitable web page or a single web site to access (Children can be locked into this on iPads);
- children may be provided with lists of relevant and suitable web sites which they may access;
- more experienced children may be allowed to undertake their own internet search having agreed a search plan with their teacher; pupils will be expected to observe the rules for 'Responsible Use of the laptops and iPads' and will be informed that checks can and will be made on the sites they access.

Children accessing the internet will be supervised by an adult, normally their teacher, at all times. They will only be allowed to use the internet once they have been taught the rules for 'Responsible Use of the laptops and iPads' and the reasons for these rules. Teachers will endeavour to ensure that these rules remain uppermost in the children's minds as they monitor the children using the internet.

In addition, parental permission must be granted before children use the internet to support their learning.

B4 Using information from the internet

We believe that, in order to use information from the internet effectively, it is important for children to develop an understanding of the nature of the internet and the information available on it. These Digital Literacy skills are important for the children now, but are also life skills which are important for the children's future. Through our school Computing Curriculum children will learn about the three main strands of the computing curriculum; Computer Science, Digital Literacy and Digital Citizenship, and develop an understanding of the nature and purpose of their digital world and how it effects their lives.

- Teachers will explicitly teach 'Digital Literacy' through the use of Project Evolve, ensuring that children 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, children will be taught to observe copyright protections (copyright and ownership strand Project Evolve);
- Where appropriate children will be made aware that the writer of an e-mail or the author of a web page may not be the person claimed (Privacy and Security strand Project Evolve)

B8 Use of iPads and Apps

Children in school will have access to iPads which have a range of appropriate, educational apps on to support learning. Each class in school will have their own seesaw account which will be accessible through staff and children's iPads. Each class will have their own QR code to access their class page however these will not be on display in the classroom and will only be given to children when necessary. Children will only be able to see work in their class which the teacher has accepted. Through the schools Computing Curriculum, children will be taught how to upload photographs from the iPad to seesaw and take photographs/videos on the app. The class teacher will have responsibility for checking work which the children post and giving feedback on this. Children will be taught how to delete photographs which they have taken on the iPads before the end of the lesson or as soon as possible thereafter.

B9 Sanctions

If the privileges of access to the internet and school IT Equipment are abused by failing to follow the rules that have been taught, then sanctions consistent with our Behaviour and Relationships Policy (refer to Behaviour and Relationship policy) will be applied. This may involve informing the parents/carers. Teachers may also consider whether access to IT facilities in school may be denied for a period. The sanctions which are likely to be applied are as follows, however individual circumstances will determine the exact sanction that would be used.

Part C- Governors, Parents and Visitors using the School Network and Computing Equipment

C1 Access to the school network for Governors, Parents and Visitors

Governors, parents and other visitors to school may need access to the school network. For example a visiting speaker may need to show a presentation on a Smartboard or use a website, a Governor may use a school PC to complete a task related to their role, or a parent helper may be making resources while helping in school. For this reason, a 'visitor' account has been set up. If use of the school network is needed, the Governor, parent or visitor will be asked to read an abbreviated version of this policy, with a full version being available on request, and if they agree to adhere to it, they will be given a user name and password. The abbreviated version of the policy will refer to the relevant sections of this policy (see below).

C2 Access to the school network for Trainee/Student Teachers

The school often hosts trainee or student teachers on placements which form part of their Initial Teacher Training (ITT). Trainee or student teachers require access to the school network as part of their teaching commitments and to complete their professional studies. Each trainee will be given an individual user name and password to enable them to access the school network and the internet. They will not be given a school email address. The account will also provide access to a network drive where they may save files. As well as subject to the monitoring described in Part A, the network drive provided will also be accessible to the Computing Subject Leader and the Headteacher for monitoring purposes.

C3 Working with children and PCs/laptops/iPads

If Governors, parents or other visitors are working with children using computers or iPads, particularly if they are using the internet, they should be made aware of the importance of e-safety and the rules children follow. If they become aware of children viewing any inappropriate content, they **MUST** inform the member of staff they are working with or the Headteacher.

C4 Taking photographs

Visitors to school may not take photographs of the children without first requesting and receiving permission from the Headteacher. Unless the Headteacher decides differently, permission is given for parents to take photographs and record videos of children performing in class assemblies, the Year 4 leavers' assembly, Christmas concerts and any other performances; this is on the understanding that these are for personal use only. Visitors will be told this very clearly in advance. Parents and carers have been told to inform school if they do not want their children to be included.

C5 Sanctions

While not subject to disciplinary procedures due to the nature of their role, any visitors who breach this policy may be subject to civil or criminal action, and they should be aware that school is obliged to report illegal activity taking place on school premises or using school equipment to the Police.

Monitoring and Review

The policy will be reviewed on an annual basis by the E-safety Committee to ensure it is appropriate in light of recommended best practice and complies with statutory regulations. In the event of any conflict with statutory regulations, the legal provisions will have precedence over this procedure in all cases.

The E-safety Committee, reporting to the Governing Body, will monitor the application of this policy and procedure, particularly to ensure that the school's practices comply with it. This will primarily take the form of an e-safety walk around school looking for good practice being observed as well as any breaches of this policy. This will take place annually, prior to refreshing e-safety training to determine where the focus of the training needs to be.

REVIEW

Last reviewed: Autumn term 2024 by Rebecca Storey

Next review: Autumn 2025

Appendix 1 : Rules for Responsible use of our school laptops and iPads for Key Stage 2, Key Stage 1 and Reception

Responsible use of our school laptops and iPads



- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will inform my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from.
- When communicating online, I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not log on using another person's account.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers.
- I understand that if I am acting inappropriately then my parents may be informed and I may not be allowed to use the computing equipment at school.



The Golden Rule:
Think before you click



Responsible use of our school laptops and iPads

The Golden Rule: Think before you click

- ☺ I will follow clear instructions from my teacher when using the internet.
- ☺ I will only use the internet when a teacher is with me.
- ☺ If I see something that upsets me, I will tell a teacher.
- ☺ I will think before I print or delete.
- ☹ I won't look at or delete other people's files.
- ☹ I won't log on using someone else's username.
- ☹ I won't complete forms on the internet or share personal information with others on the internet.

I know that if I deliberately break any of these rules, I may not be allowed to use the computers and my parents may be informed.



KS 2 Responsible use of our school laptops and iPads

- At all times, I will think before I click (especially when deleting or printing).
- When using the internet, I will think about the websites I am accessing.
- If I find a website or image that is inappropriate, I will click Hector the dolphin to cover the screen and tell my teacher straight away.
- When using information or pictures from websites, I will try and say which website it came from and if possible link back to the site.
- When communicating online, I will think about the words that I use and will not use words that may offend other people.
- When communicating online, I will only use my first name and not share personal details such as my email address or phone number.
- I understand that people online might not be who they say they are.
- I will not look at other people's files or documents without their permission.
- I will not log on using another person's account.
- I will think before deleting files.
- I will think before I print.
- I know that the teachers can, and will, check the files and websites I have used.
- I will keep my usernames and passwords secure, but I understand I can share them with appropriate people, such as my parents or teachers.
- I understand that if I am acting inappropriately then my parents may be informed and I may not be allowed to use the computers at school.

The Golden Rule: Think before you click

R and KS1 Responsible use of our school technology

- ☺ I will be careful when going on the internet.
- ☺ I will only use the internet when a teacher is with me.
- ☺ If I see something that upsets me, I will click Hector the dolphin to cover the screen and then tell a teacher
- ☺ I will think before I print or delete.
- ☹ I won't look at or delete other people's files.
- ☹ I won't log on using someone else's username.
- ☹ I won't complete forms on the internet or share personal information with others on the internet.

I know that if I deliberately break any of these rules, I may not be allowed to use the computers and my parents may be informed.

The Golden Rule: Think before you click

Appendix Two: Internet Permissions



September 2022

Dear Parents/Carers

Using the Internet at Havannah First School

Welcome to the new school year. We would like to share the following information about internet use at Havannah First School with you.

How the internet is used in school:

- We provide supervised access to the Internet as part of the whole school curriculum, including explicitly through the teaching of the Computing curriculum.
- We believe that the use of the internet is worthwhile and part of the essential skills for children as they grow up in the modern world. Classes will also use Twitter to share their learning with others.
- We have taken positive steps to minimise the risk of access to undesirable materials. This includes a filtering system and firewall provided by the Internet Service Provider. (This may not be the case at home and we can provide references to information on safe Internet access if you wish.) Children are also taught a set of rules through the delivery of our e-safety curriculum for using the computers in school responsibly, a copy of which is attached.
- In accordance with good practice, we need your permission for your child to use the internet in school.

NB Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities. A full copy of our Information Security and Acceptable Use of IT Policy is published on the school website, and a paper copy is available on request from the school office or the Computing Subject Leader.

Our school website: Use of photographs and video

- Our school website address is www.havannah.newcastle.sch.uk
- It is continually developing and is an exciting opportunity to share information about children's learning and our school, and also to promote the school to the wider community.
- We use activities completed by the children, photographs and videos of the school and activities which take place in school on the website, and these may include children. We do not publish pupils' full names or photographs that identify individuals on our web pages. A child in a photograph would never be named, unless it was in exceptional circumstances and only with parental permission. School performances may be filmed, used in school and possibly sold as a fundraising activity.
- We consider ourselves to use images responsibly and appropriately, but we need your permission to use photographs and video of your child on the website and to publish their work.
- If you have any concerns about this, please look at the school website to see how images are used and also discuss your concerns with me or another member of staff before making your final decision. It may reassure you to know that it is usually difficult to identify individuals on the website as the children mostly appear in groups, often facing away from the camera while completing an activity. Around 95% of parents agree to photos of their child being used.

The attached permission form asks for permission for:

- Your child to use the internet
- For their work to be used on the school website and Twitter
- For their photograph/video to be used on the school website and Twitter
- For their photograph to be used in the media, press and publicity materials

This permission is sought for the time your child is at Havannah First School (usually the end of Year 4). Should your wishes change during this time, please inform school of this as soon as possible.

Please complete the attached form and return it to school by xxx. If you decide not to give permission for any of the above, please inform your child's class teacher by xxx so we can ensure your wishes are fulfilled. If forms are not returned by this date, school staff will have to contact you and this wastes valuable time. Should you wish to discuss any aspect of Computing or Internet use, please telephone school to arrange an appointment with me or Ms McKenna.

Using the internet and use of images at Havannah First School

(from September 2022 until my child leaves the school)

Please sign and return this form to school by ...



NAME OF CHILD _____ CLASS _____

USING THE INTERNET

I have read and understood the school rules for Responsible Use of our School Computers.

I understand that the school will take all reasonable precautions to ensure pupils cannot access inappropriate materials, and that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

I give permission for my child to access the Internet.

Signed _____ Please print name _____

PUBLISHING WORK ON THE INTERNET

I agree that, if selected, my son/daughter's work may be published on the Internet, including the school website and Twitter.

Signed _____ Please print name _____

PUBLISHING IMAGES/VIDEOS ON THE INTERNET

I give permission for photographs/videos including my child to be published on the school website and Twitter and included in recordings of school performances.

Signed _____ Please print name _____

USE OF PHOTOGRAPHS IN MEDIA, PUBLICITY AND PRESS

We sometimes use children's photographs in the local press, training materials for schools and other institutions.

I give permission for photographs including my child to be published in the press and in other printed publications.

Signed _____ Please print name _____

Please note: We never publish photographs with full names but the press often do even when directed otherwise, therefore by giving permission to use your child's photographs in the press you must also be giving permission to use his or her names.

Appendix Three : Staff, Governor, volunteer and visitor agreement

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:	
<ul style="list-style-type: none"> • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms (on school ICT Systems or devices) • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school 	
<p>I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.</p> <p>I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.</p> <p>I will let the designated safeguarding lead (DSL) and Computing Lead know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.</p> <p>I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.</p>	
Signed (staff member/governor/volunteer/visitor):	Date: