



Grange Primary School

Pursuing excellence for every child

Grange Primary School

**Internet and Digital Technology
Acceptable Use Policy**

2025

Date Reviewed: March 2025

Next Review: March 2026

Table of Contents

<i>Table of Contents</i>	2
<i>Relevant legislation and guidance</i>	3
<i>Acceptable Use Statement</i>	4
<i>Acceptable use of IT Equipment</i>	4
<i>Purpose of the Policy</i>	4
<i>Guidelines</i>	4
<i>General Conditions</i>	5
<i>Data Security</i>	5
<i>Anti-Virus and Firewall Security</i>	6
<i>Physical Security</i>	6
<i>Access To Google Drive</i>	7
<i>Breaches of this Policy</i>	7
<i>Use of telephones, email and internet by staff</i>	9
<i>Safe use of online resources</i>	11
<i>Personal Devices</i>	11
<i>Password Policy</i>	12
<i>Questions, Complaints and Appeals</i>	12
<i>Software</i>	12
<i>Further guidelines</i>	13
<i>Visitors and volunteers</i>	13
<i>The Acceptable User Agreement – Members of staff</i>	14
<i>Acceptable Use Policy – Pupils</i>	15
<i>The Acceptable User Agreement – Pupils</i>	17
<i>Ratification</i>	19

Relevant legislation and guidance

This policy refers to, and complies with, the following legislation and guidance:

[Data Protection Act 2018](#)

[The General Data Protection Regulation](#)

[Computer Misuse Act 1990](#)

[Human Rights Act 1998](#)

[The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)

[Education Act 2011](#)

[Freedom of Information Act 2000](#)

[The Education and Inspections Act 2006](#)

[Cyberbullying: Embedding Anti-Bullying Work in Schools. \(DCSF 2007\)](#)

[Keeping Children Safe in Education 2021](#)

[Searching, screening and confiscation: advice for schools](#)

[National Cyber Security Centre \(NCSC\)](#)

[Education and Training \(Welfare of Children Act\) 2021](#)

Acceptable Use Statement

Acceptable use of IT Equipment.

1. Grange Primary School is committed to safeguarding its IT infrastructure to ensure it can be used in the most effective manner to support teaching and learning and all necessary administrative processes. Ensuring the safety and integrity of the school IT infrastructure is the responsibility of all staff. The school encourages use in a responsible and professional manner. Portable computers include for example laptops, tablets and other portable IT devices where provided. As a user of IT services of the school you have a right to use its computing services; that right places responsibilities on you as a user which are outlined below. If you misuse school computing facilities in a way that constitutes a breach or disregard of this policy, consequences associated with that breach may apply to you, and you may also be in breach of other school regulations. Ignorance of this policy and the responsibilities it places on you is not an excuse in any situation where it is assessed that you have breached the policy and its requirements.
2. Staff are advised of this policy during their induction and of the requirement for them to adhere to the conditions therein. For the purposes of this policy the term "computing services" refers to any IT resource made available to you, any of the network services, applications or software products that you are provided access to and the network/data transport infrastructure that you use to access any of the services (including access to the internet). Staff who connect their own IT to the school network and the services available (where permitted) are particularly reminded that such use requires compliance to this policy.

Purpose of the Policy

- To protect the school networks and equipment
- To protect the school data
- To protect the school and its employees from activities that might expose them to legal action from other parties

Guidelines

Password Security

Access to systems and services is controlled by a central computing account and password. Staff are allocated their User ID and initial password as part of their induction with the school. User IDs and passwords are not to be shared or revealed to any other party. Those who use another person's user credentials and those who share such credentials with others will be in breach of this policy. Initial default passwords issued to any user should be changed immediately following notification of account set up. Passwords should be changed immediately if the user believes or suspects that their account has been compromised. Management and IT support should also be notified if a compromise takes place or is in any way suspected.

General Conditions

Use of school "computing services" should be for research, teaching or the administrative purposes of the school.

- Your use of the school computing services must at all times comply with the law.
- Your use of the school computing services must not interfere with any others' use of these facilities and services.
- You are not entitled to use a computer that you have not been authorised to use.
- You must not access any program or data which has not been specifically authorised for your use.
- You must not use or copy any data or program belonging to other users without their express and specific permission.
- You must not alter computer material belonging to another user without the users' permission.
- You must not use school computing services to harass, defame, libel, slander, intimidate, impersonate or otherwise abuse another person.
- You must not use school computing services for the creation, collection, storage, downloading or displaying of any offensive, obscene, indecent or menacing images, data or material capable of being resolved into such. (There may be certain legitimate exceptions for educational purposes which would require the fullest disclosure and special authorisation from the Head).
- You must not use the school computing services to conduct any form of commercial activity without express permission.
- You must not use the school computing services to disseminate mass (unsolicited) mailings.
- You must not install, use or distribute software for which you do not have a licence, and which is not first authorised by the IT Department for installation.
- You must not use any peer-to-peer file sharing software without the express written permission of the IT manager.
- You must not use any IRC or messenger software including, but not limited to AOL, MSN, Yahoo! or other "Messengers", IRC or "chat" clients unless expressly authorized to do so for work related purposes.
- You must not use any form of network monitoring which will intercept data not specifically intended for you unless this activity is a part of your normal job responsibilities or has been specifically authorised by the Headteacher/Governing Body

This policy aims to provide a summary of the guidelines for staff, but is by no means exhaustive. In adhering to the spirit of this document as well as the rules herein, staff will be able to use the network at Grange Primary School in a safe and responsible way.

Data Security

The school holds a variety of sensitive data including personal information about students and staff. If you have been given access to this information, you are reminded of your responsibilities under data protection law. You should not take a copy of data outside the school systems. This includes sending a file or folder to a personal email address or any other email address that is not strictly for work purposes, putting sensitive data onto laptops,

memory sticks, CDs/DVDs, and any portable. If you do need to take data outside the school, this should only be with the authorisation of the school Data Protection Officer and follow comply with the Data Protection policy.

The school makes use of the Google Drive to share files and folders across the organisation. Staff members access the Google Drive through their secure username and password. When the Google Drive is accessed off-site, the user must ensure that it is only ever on a school-owned laptop or IPAD and never a personal device.

Anti-Virus and Firewall Security

All personal computers are installed with current versions of virus protection and firewall software (where necessary) by the IT Department. Users are not to alter the configuration of this software. This software is installed to prevent an attack from malicious software and to prevent loss of data and corruption of programs/files. Users must shut down their computer at the end of each day to ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, they should inform the Computing Lead or Head teacher immediately. If the IT Technical Support detects a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe, and must remain unused until reinstated by the IT support staff.

Physical Security

The users of IT equipment should always adhere to the following guidelines:

- Treat equipment safely, in the same manner as a reasonable person would
- Keep liquids away from IT equipment
- Do not place heavy objects on IT equipment
- Do not drop IT equipment or objects onto it
- When taking laptops home they should always be in a computer case.
- Any portable computer must be securely locked away when not in use.
- Portable computer security is your responsibility at all times- Do not leave the portable computer unattended in a public place or within the school
- Do not leave the portable computer on view inside your car. It should be locked away in your car out of sight.
- Extra reasonable care must be taken to prevent the loss of any portable media which contain confidential school data, and any portable data storage devices must be encrypted.
- Staff supervising pupils using IT equipment should ensure pupils take reasonable care of such equipment.
- In the event a portable computer is damaged or lost as a result of non-compliance with this policy or as a result of other negligent action, then you must inform the Head teacher as soon as possible and you may be required to make a full or partial contribution towards any reparation/replacement costs, at the discretion of the school.

Access To Google Drive

- Grange Primary School uses Google to provide our email and data storage.
- All teachers have access to a personal google drive and should use this to store files and folders that are needed for performing their duties at work.
- The Google Shared Drives should be used to store data, folders and files that need to be accessed by others.
- Where the Shared Drive is accessed at home, the member of staff must ensure that they only use a school-owned device.
- Staff should not delete files or folders on the Google Shared drive unless they have agreement from their whole team.

Breaches of this Policy

Incidents which are determined to be in contravention of this policy will be assessed for their severity. Investigating such incidents may require the collection and evaluation of user related activity and evidence. It is not possible to provide an exhaustive list of potential ways in which a user may contravene this policy but in general such breaches will be categorised into one of three levels of severity and each level of breach will carry with it a possible range of sanctions, consequences and/or penalties.

Minor Breach

This level of breach will attract a verbal warning which will be held recorded for 12 months. In general this category will relate to behaviour or misuse of computer facilities that can be characterised as disruptive or a nuisance. Examples of this level of non-compliance would include:

- Taking food and/or drink into IT facilities where they are forbidden.
- Sending nuisance (non-offensive) email
- Behaving in a disruptive manner. Not all first offences will be automatically be categorised at this level since some may be of a significant or impact that elevates them to one of the higher levels of severity.

Moderate Breach

This level of breach will attract more substantial sanctions and/or penalties. Examples of this level of non-compliance would include:

- Repeated minor breaches within the above detailed 12 month period.
- Unauthorised access through the use of another user's credentials (username and password) or using a computer in an unauthorised area.
- Assisting or encouraging unauthorised access.

- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering or libelling another person.
- Misuse of software or software licence infringement.
- Copyright infringement.
- Interference with workstation or computer configuration.

Severe Breach

This level of breach will attract more stringent sanctions, penalties and consequences than those above, and access to computing facilities and services may be withdrawn (account suspension) until the disciplinary process and its outcomes have been concluded. Examples of this level of breach would include:

- Repeat moderate breaches.
- Theft, vandalism or wilful damage of/to IT facilities, services and resources.
- Forging email i.e. masquerading as another person.
- Loading, viewing, storing or distributing pornographic or other offensive material.
- Unauthorised copying, storage or distribution of software.
- Any action, whilst using school computing services and facilities deemed likely to bring the school into disrepute.
- Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy IT systems security.
- Attempting to modify, damage or destroy another authorised user's data.
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities. Attempting unauthorised access to a remote system.
- Attempting to jeopardise, damage circumvent or destroy IT systems security.
- Attempting to modify, damage or destroy another authorised user's data.
- Disruption of network communication capability or integrity through denial of service attacks, port scanning, monitoring, packet spoofing or network flooding activities.

Process

An investigation will be carried out, in confidence, by school leadership under the direction of the Headteacher, to be considered within the school disciplinary procedures. Each set of disciplinary procedures provide for an appeal stage.

Use of telephones, email and internet by staff

Principles

The provisions of this Policy apply to all members of staff, whether or not they have access to, or sole use of, a telephone or e-mail/the Internet on a personal computer. Although access to such facilities does not form part of the benefits provided to staff, it is recognised that there are occasions when employees might legitimately make private use of these facilities. This policy is intended to make clear what constitutes legitimate use. It is intended not to place employees under unjustifiable scrutiny, but to give them a high measure of security and confidence about their use of e-mail, telephones and the internet. The sections of the policy covered by misconduct and misuse should be read in conjunction with the appropriate staff disciplinary procedure. This policy has been designed to safeguard the legal rights of members of staff under the terms of both the Data Protection Act and the Human Rights Act.

Purposes

To provide guidance on inappropriate use of school telephones, email and internet facilities.
To clarify when the school may monitor staff usage of these facilities.

Use of telephones

There will be occasions when employees need to make short, personal telephone calls on school telephones or personal mobile phones in order to deal with occasional and urgent personal matters. Where possible, such calls should be made and received outside the employee's normal working hours or when they do not interfere with work requirements.

When awaiting particularly pressing, sensitive or urgent information by mobile phone, members of staff may be permitted to keep their phone about their person. This **must** be agreed with either the Head or Deputy in advance. It is understood that the member of staff still ensures that their safe-guarding duties are met for any children that they are responsible for and does not leave the rest of the class under-ratio or in a position of danger by taking the call.

The use of school telephones for private purposes, which are unreasonably excessive or for school purposes which are defamatory, obscene or otherwise inappropriate, may be treated as gross misconduct under the appropriate disciplinary procedure. Where the school has grounds to suspect possible misuse of its telephones, it reserves the right to audit the destination and length of out-going calls and the source and length of in-coming calls. This would not normally involve the surveillance of calls but in certain rare circumstances where there are reasonable grounds to suspect serious misconduct, the school reserves the right to record calls.

Use of email

As with telephones it is recognised that employees can use e-mail for personal means in the same manner as that set out for telephones above. E-mail should be treated like any other form of written communication and, as such, what is normally regarded as unacceptable in a letter or memorandum is equally unacceptable in an e-mail communication. Employees should be careful that before they open any attachment to a personal e-mail they receive,

they are reasonably confident that the content is in no sense a risk to security, obscene or defamatory to avoid contravening the law. Equally, if an employee receives an obscene, compromised in terms of security, or defamatory e-mail, whether unwittingly or otherwise and from whatever source, s/he should not intentionally forward the e-mail to any other address, unless specifically requested to do so by an investigator appointed by the school. Any suspicious attachments to email or indeed any website or software which requests login details should not be used until verified safe by the IT support department. Any other use of e-mail for either personal or school purposes to send or forward messages or attachments which are in any way defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure. Where the school has reasonable grounds to suspect misuse of e-mail in either scale of use, content or nature of messages, it reserves the right to audit the destination, source and content of e-mail to and from a particular address. The school also reserves the right to access an employee's e-mail account in her/his unexpected or prolonged absence (e.g. due to sickness) in order to allow it to continue to undertake the employee's normal role. In normal circumstances the employee concerned will be contacted before this is done, in order to provide him/her with prior knowledge.

Use of the Internet

The primary reason for the provision of internet access is for the easy retrieval of information for educational purposes, or to make use of learning resources, or to make legitimate authorised purchases to enhance the ability of its staff to undertake their school role. However, it is legitimate for employees to make use of the internet in its various forms in the same way as email above as long as it is not used to view or distribute improper material such as text, messages or images which are derogatory, defamatory or obscene. Members of staff must only use an authorised school device to access the internet. Personal devices must not use the wifi within school as this represents a risk to the security of the school network. Unauthorised use of the internet, which is unreasonably excessive for personal use or for purposes which are defamatory, obscene or otherwise inappropriate will be treated as gross misconduct under the appropriate disciplinary procedure.

The school uses filtering software – Cisco Meraki- provisioned by Education Lincs and monitored by the DSL and Online Safety Officer. (**Also see Online Safety Policy and Social Media Policy**)

Monitoring the use of telephone, e-mail and the Internet.

It is not school policy, as a matter of routine, to monitor an employee's use of the school telephone or e-mail service or of the internet via the school networks. However, as has been stated, where there are reasonable grounds to suspect an instance of misuse or abuse of any of these services, the Headteacher or Governing Body may grant permission for the auditing of an employee's telephone calls e-mail or use of the internet. Once approved, the monitoring process will be undertaken by the Headteacher. The strictest confidentiality will be adhered to when undertaking these activities and they will monitor only to the extent necessary to establish the facts of the case to enable human resources to advise the appropriate actions that may need to be taken in any particular case. When monitoring is approved, the case for continued monitoring shall be reviewed on a regular basis with a view to terminating monitoring in as short a period of time as possible.

Safe use of online resources

Principles

This applies to all online/intranet resources provided by Grange Primary School, for example Arbor.

Purposes

Security

This Policy is intended to minimise security risks. These risks might affect the integrity of Grange Primary School data. In particular, these risks arise from:

- The intentional or unintentional disclosure of login credentials
- The wrongful disclosure of private, sensitive and/or confidential information

Data Access

This policy aims to ensure all relevant aspects of the Data Protection Act (1998) and Fair Processing Policy are adhered to.

- This Policy aims to promote best use of systems to further the communication and freedom of information between Grange Primary School and Parents/Carers.
- In addition, data processing should at all times comply with and be compliant to the conditions of GDPR

Guidelines

Grange Primary School online systems are provided for use only by persons who are legally responsible for pupil(s) currently attending the school. Access is granted only on condition that the individual formally agrees to the terms of this and any other relevant policy. The authorising member of Grange Primary School staff must confirm that there is a legitimate entitlement to access information for pupils. A copy of the form will be held by the school for audit purposes.

Access to school MIS from home

Only those with express permission may access our MIS – Arbor – from home. Two-factor authentication will be required to gain access outside of the school building. This will be given at the discretion of the Head to the following post holders: DSL, Deputy DSLs and Deputy Head teacher.

Personal Devices

For work-use: no Grange School data may be stored locally on personal devices. All systems must be used securely, must not be left logged in and unattended, and must comply with all relevant security and online safety policies whilst in use. Users must ensure they are logged out of any Grange Primary School systems as soon as any work activities are finished.

For non-work use: Personal devices are not banned from the school premises but must be on silent or on 'do not disturb' and comply with the School's **Online Safety policy**.

Best practice is not to access the system in any environment where the security of the information contained may be placed at risk.

Password Policy

Staff must assume personal responsibility for usernames and passwords. Never use anyone else's username or password. You must always keep your individual user name and password confidential. These usernames and passwords should never be disclosed to anyone. Passwords and user names should never be shared. These passwords should be changed when any breach of secrecy is suspected or proven. IT support or line management should be informed of any such breach. Where passwords are prescribed for users or for services, IT support (or line management or relevant member of staff) should be informed immediately should a change be required or breach occurs.

Questions, Complaints and Appeals

Users should address any complaints and enquiries about the system to The Headteacher. Where availability or concerns pertaining to data processing arise, these must be directed to the Data Protection Officer. Grange Primary School reserves the right to revoke or deny access to MIS systems of any individual under the following circumstances:

- The validity of parental/carer responsibility is questioned
- Court ruling preventing access to child or family members is issued
- Users found to be in breach of this policy

If any child protection or Safeguarding concerns are raised or disputes occur Grange Primary School will revoke access for all parties concerned pending investigation.

Please note: Where MIS access is not available School will still make information available according to Data Protection Act (1998) law.

Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

Software

Software should be purchased or acquired from reputable vendors, in all cases following approval preferably in writing from the Head/Deputy teacher. Installation of any software (where staff have rights to do so) must be approved by the Head/Deputy; no software may be installed by staff alone. Breach of this condition represents a large security and data protection risk, and may be grounds for disciplinary action.

Further guidelines

Staff must not:

- create, transmit or cause to be transmitted any threatening material, material which breaches copyright, material likely to cause damage, offend, distress, cause anxiety to or prevent another user from carrying out their duties
- cause a computer or another user of the network to access unauthorised data (secured or unsecured)
- impair the operation of a computer either deliberately or recklessly
- act in a way that would cause or create risk of damage to physical IT systems or data
- create, supply or obtain articles (including but not limited to software and data) for use in the above and following items
- partake in activity defined as Cyber-dependent crimes and/or Cyber-enabled crimes (see CPS http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a23 and CPS http://www.cps.gov.uk/legal/a_to_c/cybercrime/#a24)
- access, store, transmit or possess pornographic, terrorist/extremist, illegal or unprofessional material and/or data relating to the aforementioned

Visitors and volunteers

Whilst it won't be necessary for all visitors and volunteers to sign this/ an Acceptable Use Policy, it is important that Grange Primary School representatives provide regular visitors and volunteers with clear expectations regarding online behaviour and confidentiality. If you arrange for/ are responsible for a visitor or volunteers who may need to sign an AUP please ensure that the **visitor has read and signed the Acceptable Use Policy for Visitors and that when this is done and the document is dated and retained.**

This Acceptable Use Policy can therefore help ensure that clear information regarding the settings expectations regarding online conduct is provided; this is especially important to ensure confidentiality policies are respected. For example, a concern could arise if a parent volunteer posted comments on social media about another child's behaviour. There will also be situations whereby visitors and volunteers may need to have access to or use settings systems and/or data, such as governors, visiting IT staff or external speakers. It is important that, if you are responsible for or have invited a visitor, clear expectations are put in place regarding appropriate access and behaviour prior to access being permitted.

The Acceptable User Agreement – Members of staff

All adults within the school must be aware of their safeguarding responsibilities when using any online technologies, such as the internet, E-mail or social networking sites. They are asked to sign this Acceptable Use Agreement so that they provide an example to children and young people for the safe and responsible use of online technologies. This will educate, inform and protect adults so that they feel safeguarded from any potential allegations or inadvertent misuse themselves.

The school has a code of conduct drawn up to protect all parties – the pupils, the staff and the school. To ensure members of staff are fully aware of their professional responsibilities when using information systems and when communicating with pupils, they are asked to sign this code of conduct. Members of staff should consult the school's Internet-safety policy for further information and clarification:

- I understand that it is a criminal offence to use the school computing system for purpose not permitted by its owner.
- I appreciate that Computing includes a wide range of systems, including mobile phones, digital cameras, email, social networking and that Computing use may also include personal Computing devices when used for school business.
- I understand that the school information systems may not be used for private purposes without specific permission from the Headteacher.
- I understand that use for personal financial gain, gambling, political purposes or advertising is forbidden.
- I understand that my use of school information systems, laptops, Chromebook Ipads, Internet and email may be monitored and recorded to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager.
- I will not allow another member of staff or visitor to use my login details to access the school systems.
- I will not install any hardware or software without permission.
- I will ensure that personal data is stored securely and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I understand that my use and storage of photographic images or video recordings of pupils taken in school or on school activities should be compatible with my professional role and should be done on school owned equipment.
- I will respect copyright and intellectual property.
- I will report any incidents of concern regarding children's safety to the DSL (Designated Safeguarding Leader)
- I will ensure that electronic communications with pupils including e-mail are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I understand that I must not communicate with current or former students of the school using public social networking sites (e.g. Facebook) and that if contact with students is required, I must use school-owned equipment or facilities (e.g. the email facility or a phone provided by the school).
- I will promote Internet-safety and Digital Citizenship with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.

I have read, understand and accept the Staff Code of Conduct for Computing.

Signed.....
school.....

Accepted by

Printed Name.....
Date.....

Acceptable Use Policy – Pupils

Children must not use the school digital facilities without the supervision of a member of staff. Although use of the digital facilities and access to the Internet will be supervised and all possible measures will be taken, Grange Primary School cannot accept liability for the accessing of inappropriate materials or any consequences of internet access.

If staff or children discover unsuitable sites, the URL (address) and content must be reported to the Computing Leader immediately who will, in turn, record the address and report on to the Head Teacher or Internet-Safety leader.

Children are aware that they must only access those services they have been given permission to use. Staff and children are made aware that the use of computer systems without permission or for inappropriate purposes is prohibited in school.

Children and parent(s)/carer(s) must agree to and sign the Acceptable Use Agreement on entry to the school.

Log in and Passwords

- Children must not disclose any password or login name given to anyone or allow anyone else to use a personal account.
- Children must not attempt to gain access to the school network or any Internet resource by using someone else's account name or password.
- Children must ensure that all laptops or Chromebooks are logged off (or locked) when left unattended.

General Safety and Risk Assessment

The consumption of food or drink is forbidden whilst using a computer. It is hazardous to the equipment and to individuals.

Users must treat equipment and services in school and at other sites accessed through school facilities with respect and are subject to regulations imposed by the respective service providers. Malicious action will result in immediate suspension from use of the school facilities. Staff are responsible for sharing safety issues with their children. Staff are responsible for the care of their iPad and/or computer; including the transportation and use of equipment at members of staffs' homes.

Cyber Bullying

The experience of being cyber bullied can be very painful for those who are the targets. Adults need to help children and young people prepare for the hazards of using technology while promoting learning and social opportunities. Some forms of cyber bullying are different from other forms:

- Through various media children can be cyber bullied 24 hours a day
- People who cyber bully may attempt to remain anonymous
- Anyone of any age can cyber bully
- Some instances of cyber bullying may be unintentional – such as a messages sent as a joke or an email to the wrong recipient

Prevention of Cyber Bullying

We recognise that the best way to deal with cyber bullying is to prevent it from happening in the first place. By embedding good, safe practice into all our teaching and learning, incidents can be avoided.

We recognise that we have a shared responsibility to prevent incidents of cyber bullying. The Head Teacher has the responsibility for coordinating and monitoring the implementation of anti-cyber bullying strategies.

Understanding Cyber bullying

The school is aware of the definition of cyber bullying and the impact cyber bullying has. Staff receive guidance and review the Anti-Bullying policy and Acceptable Use Policy regularly. Children are taught how to recognise cyber bullying and their responsibilities to use digital technologies safely. IT safety is integral to teaching and learning practice in the school.

Personal mobile devices and smart watches

Children are prohibited from bringing mobile devices including mobile phones, tablets, cameras and smart watches, on to school premises. Such devices, could compromise the safety of the children and should not be brought in to school. Please see the School Uniform Policy for more details.

The Acceptable User Agreement – Pupils

The school has installed computers with internet access to help our learning. These rules will help keep us safe and help us be fair to others. Remember to always be kind!

Using the Computers, Chromebooks and iPads:

- I will only access the computer system with the login and password I have been given;
- Try my hardest to remember my username and password. If I forget my password, I will let my teacher know.
- Never share my password with anyone, including my friends.
- Never give my personal information (my name, address or telephone numbers) online to anyone without the permission of my teacher or parent/carer and let my teacher know if anybody asks me for my personal information.
- I will not use other people's username or passwords to access any other services provided by the school.
- I will not bring in memory sticks from outside school and try to use them on the school computers.
- I will use the equipment responsibly and for the task that has been set.
- If I am unsure of anything during a lesson, I will speak to a member of staff immediately.
- I will treat all digital equipment in school with care.
- Not use other people's work or pictures without permission to do so.
- Be respectful to everybody online, I will treat everybody the way that I want to be treated, be kind to others and not upset or be rude to them and let my teacher know if anybody says or does anything to me that is hurtful or upsets me.
- Handle the equipment carefully, if I accidentally damage something or if it is not working properly I will tell my teacher straight away.
- not download anything from the internet unless the teacher has asked me to.
- only play games my teacher has asked me to and not play on games unsuitable for my age.
- not access social media sites or apps that are not suitable for my age.
- Log off and shut down a computer when I have finished using it.
- I understand – that some people on the internet are not who they say they are, and some people can be nasty.
- I understand – that the school will monitor the websites I visit and if I break the rules in this charter there will be consequences of my actions.

Using the Internet:

I will follow the SMART rules set out below while on the internet:

1. **Safe** – I will keep safe by being careful not to give out personal information when I'm chatting or posting online. Personal information includes my email address, phone number and password.
2. **Meeting** – I will not meet someone I have only been in touch with online because this can be dangerous. I will only do so with my parents' or carers' permission and even then only when they can be present. Remember online friends are still strangers even if you have been talking to them for a long time.
3. **Accepting** – I will not accept emails, IM messages, or open files, pictures or texts from people I don't know or trust because this can lead to problems – they may contain viruses or nasty messages!

4. **Reliable** – I understand someone online might lie about who they are and information on the internet may not be true. I will always check information with other websites, books or someone who knows. If I like chatting online it's best to only chat to my real world friends and family

5. **Tell** – I will tell my parent, carer or a trusted adult if someone or something makes me feel uncomfortable or worried, or if I or someone I know is being bullied online.

Please sign below to indicate that you agree to the Acceptable Use Policy for Internet use for yourself and your child.

Be Kind online:

I am aware that it is completely unacceptable to be mean to others online. If I am involved in cyber-bullying of any kind, I will have to face up to sanctions such as losing my rights to use school devices.

If I feel that someone has been unkind to me, I know that I can talk to my teacher or other trusted adult around the school.

I will always let a teacher know if I see someone being unkind when using a school device.

Parent/Carer signature.....

Year	Signed	Date
R		
1		
2		
3		
4		
5		
6		

Ratification

Date ratified by the Governing Body: March 2025

Date last reviewed: March 2024

Next review date: March 2026

Virtually Signed by Chair of Governors: Mr S. Ryley **Date:** March 2025