




Nether Hall School

ACCEPTABLE USE POLICY

Policy Date:	September 2023	Policy Review Date:	September 2025
Responsible Person:	Helen Robinson		
Sarah Naylor Headteacher	Signature: 	Date:	1/10/2024
Adrian Keene Chair of Governors	Signature: Not Required	Date:	

Acceptable Use Policy for all staff, governors and volunteers (referred to hereafter as staff)

Nether Hall School has provided digital technology for use by staff as an important tool for teaching, learning and administration of the school. Use of school digital devices is governed at all times by the following policy. Please ensure that you understand your responsibilities under this policy.

The purpose of the policy is to ensure the school network is operated safely and all users of digital technologies are safe. It refers to our school ICT network and to the use of mobile technologies within it and explains the behaviours, which are acceptable and unacceptable within our school.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Our AUP must be fully complied with at all times. All users of the school network should note that it is continually monitored and filtered using Netsweeper and all incidents are immediately reported to Lead and Deputy DSLs. Any person who is found to have misused the school system or not followed our AUP could face the following consequences:

- Temporary or permanent withdrawal from the school system
- Suspension from the school
- Disciplinary action
- In the most serious cases, legal action may also be taken.

Whilst our network and systems are organised to maintain the most secure environment possible **it is your responsibility to make sure the children you are directly working with are safe** when using devices and working on the network and online.

As an adult working in school you may be the first point of contact in dealing with incidents of misuse or abuse of digital equipment. Every such incident must be reported using the online-safety incident log (W:\CPOMS Injury, PI & e-safety forms\e-safety) and CPOMs. In the case of criminal activity, the Head Teacher / Lead DSL must be informed immediately.

Staff key responsibilities are:

- Maintaining an appropriate level of professional conduct in your own internet use within school.
- Developing and maintaining knowledge of internet safety issues, particularly with regard to how they might affect children.
- **Taking full responsibility for pupils' safe internet use in school.**
- Implementing our school AUP through effective classroom practice.
- Reporting any instances of digital device misuse / concerns about a pupil and their online safety immediately to a DSL.
- Supporting pupils using digital technology and online content.
- Using the internet and digital devices to ensure that online safety is not compromised e.g. evaluating websites in advance of classroom use, using child orientated search engines and ensuring pupils are only using pupil logins.
- Ensuring the security of sensitive data associated with the school, it's pupils and staff.
- Embedding online safety messages to pupils wherever possible.

School ICT Network

The school Network and associated services may be used for lawful purposes only.

Passwords

- Each child and adult working within the school must log on to the computers using the username and password given to them (class account or individual account). Passwords need to be kept confidential.
- **It is forbidden to use other adult's login details and for pupils to use staff logins.**
- Guest logins are provided for temporary staff / visitors.

Software and Downloads

- If users need a new program installing onto a digital device, our ICT Technician will be asked to do this, if possible. Do not install software on to school digital devices without permission.
- Copyright and intellectual property rights must be respected when downloading from the internet.

Personal Use

- Digital devices provided to staff are for the sole use of Nether Hall school staff. Please remember school devices off-site are monitored through the VPN network. Personal use is permitted at the discretion of the school and can be limited or revoked at any time. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden and no use of equipment may damage the school's reputation.
- School digital devices must not be used for any commercial purpose or gain unless explicitly authorised by the school.

Email / Arbor Email communication

- All members of staff with a computer login account in school are provided with a school email address for communication both internally and with other email users outside of school.
- Members of staff (including governors and non-teaching staff) must not use non-school email accounts for any school/work related activity. ~~Exceptional circumstances may be allowed at the discretion of the Head Teacher.~~
- Users are responsible for e-mail they send and should be aware that these are open to be read and should be treated as public documents.
- Email attachments of a sensitive nature must be password protected.
- Pupil's personal data must not be sent via unsecured email.
- All staff are made aware that email is not guaranteed to be private. Messages relating to or in support of illegal activities will be reported to the authorities. Anonymous messages are not permitted.
- E-mail should be written carefully, politely and professionally and should never contain anything which is likely to cause annoyance, inconvenience or needless anxiety. Anonymous messages and chain letters must not be sent.
- When writing emails, you should use appropriate professional language. You should not use language that could be considered to be inciting hatred against ethnic, religious or other groups. You need to remember that you are a representative of the school on a global public system. Illegal activities of any kind are strictly forbidden.
- All emails both sent and received will be scanned by monitoring and filtering software.
- E-mail attachments should only be opened if the source is known and trusted.
- Nether Hall school pupils are not permitted under any circumstances to e-mail a member of staff using their personal e-mail address. In addition, members of staff should not email children using their personal email address.
- Privacy – staff will not reveal any personal information (e.g. name, address, age, telephone number, social network details) of other users to any unauthorised person. Staff will not reveal any personal information to the pupils.
- Ensure that all login credentials (including passwords) are not shared with any other individuals, displayed or used by any other individual.
- In unsecured areas of school, after using a digital device, log it off immediately to safeguard pupils.
- Any unsuitable communications received must be reported to a member of SLT immediately.

Images/Videos

- All children need parental permission to have photographs or videos published electronically or in a public place or medium.
- Do not publish photographs or videos externally that identify the pupil by name at Nether Hall.
- No photos or videos which include illegal, obscene or inappropriate actions are permitted to be taken or downloaded under any circumstance.

Video conferencing

Video conferencing enables users to see and hear each other between different locations. Video conferencing may be used to support home learning, for parents /carers and pupils to attend meetings and to join in with school activities such as assemblies and performances.

To use video conferencing safely staff will ensure: -

- Parents / carers consent has been obtained prior to pupils taking part in video conferences outside of the school network.
- All video conferencing equipment in the classroom is switched off when not in use and not set to auto answer.
- External IP addresses are not made available to other sites.
- Video conferencing contact information is not accessible from the school website.
- Unique logon and password details, for the educational video conferencing services, are only issued to members of staff and kept secure
- Be situated in a public area, wearing suitable clothes and maintaining the code of conduct expected in school.

Network Protocol

- School computer and Internet use must be appropriate to a pupil's education or to staff professional activity.
- Respect other people's material and do not corrupt, interfere with or destroy them.
- Do not record, store, or distribute material without permission.
- When working with personal data ensure that the data is secure and usage follows GDPR guidelines.

Internet Usage

- Pupils must be supervised at all times when using the internet. The majority of pupils will be closely supported when online. Pupils will be taught when using the Internet to 'Stop and Tell' if concerned about any content they see or read.
- When searching the internet with pupils, staff should encourage the children to use 'child safe' search engines. However safe search is set on all computers in school as a default on search engines.
- Ensure iPads cannot access the internet if pupils are using them without direct supervision.
- The use of social networking sites and messaging systems (e.g. Facebook, WhatsApp, Twitter) is not allowed for personal use in school. Public chat rooms are not allowed. Staff and pupils may access professional forums where appropriate.
- The use of the internet from any school device for personal financial gain, gambling, political purposes or advertising is forbidden.
- No deliberate attempt will be made to visit websites that may be considered inappropriate or illegal. Staff are aware that downloading some material is illegal and that the police or other authorities may be called to investigate.

Use of Social Networking Sites and Online Forums

Staff must take care when using websites such as Facebook, Twitter, Dating Sites etc, even when such use occurs in their own time on their own digital devices at home. Social Networking sites invite users to participate in informal ways that can leave staff open to abuse, and often make little or no distinction between adult users and children.

Staff must not allow any pupil to access personal information they post on a social networking site. In particular:

- Do not add a pupil to your 'friends list', nor invite them to be friends with you.
- Ensure that personal information is not accessible via 'Public' setting, but ensure it is to a 'Friends only' level of visibility.
- Avoid contacting any pupil privately via social networking site, even for school-related purposes.
- Take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them to access to your personal information.

It is advised not to accept invitations from the pupils' parents or carers to add staff as a friend to their social networking sites, nor should staff invite them to be friends. Damage to professional reputations can inadvertently be caused by quite innocent postings or images. Staff need to ensure that any private social networking sites/blogs created or actively contributed to are not confused with their professional role in school.

Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.

- Unless authorised to do so, do not post comments on websites that may appear as if you are speaking for the school.
- Do not post any material online that can be clearly linked to the school that may damage the school's reputation.
- Avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass or defame the subject.

Use of your own Equipment

- Any mains-operated personal computer or electrical equipment brought on site, directly plugged into the mains, is subject to a Portable Appliance Test (PAT), and must not be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
- Staff must not connect personal computer devices to school computer devices without prior approval from the ICT Technician, with the exception of virus checked encrypted storage devices such as USB memory sticks. VPN access to the school network is provided for teaching staff, however, it is recognised that issues with connectivity for some staff may result in the use of encrypted memory sticks.

Mobile Devices

- Personal mobile phones should not be used in areas of school where pupils have access.
- During teaching time, mobile phones should be turned off or put on silent mode and stored in a cupboard or locker away from the children.
- Adults are allowed to access their personal phones at lunch times and during non-contact time breaks (e.g. during a training session) in suitable places where the children are not present.
- It is forbidden to take photographs/videos of the children on personal mobile phones. Any exceptions must be agreed by both the Head Teacher and parent.
- No images of the children should be taken without parental consent using any mobile device e.g. phones, school cameras. These devices must not be removed from the school premises if they contain images of pupils and without permission from a member of SLT.
- Pupils' images, whose parents have signed no publicity, will not be used on any materials, published by the school and distributed externally.

Supervision of Pupil Use

- Pupils must be supervised at all times when using school computer equipment.
- Supervising staff are responsible for ensuring that pupils use digital devices safely.
- Supervising staff must ensure they have read and understand the separate guidelines on Online-safety, which pertains to the child protection issues of computer use by pupils.

Reporting Problems with the Computer System

It is the job of the ICT Technician to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible.

- Staff should report any problems that need attention to ICT Technician via the helpdesk. This is an icon (?) on the desk top, If you can't access the icon then please use: <https://desk.ekte.uk/portal/en-gb/newticket?>
- If you suspect your computer has been affected by a virus or other malware, you must report this to the ICT Technician / helpdesk immediately.

- If you have lost documents or files, you should report this as soon as possible via the helpdesk.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. Staff must immediately inform the ICT Technician and the Head Teacher of abuse of any part of the computer system using the online safety incident log.

In particular, you should report:

- Any websites accessible from within school that you feel are unsuitable for staff or pupil consumption.
- Any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc. Do not delete the material but note the location.
- Any breaches, or attempted breaches, of computer security.
- Any instance of safeguarding concern with a pupil, bullying or harassment suffered by you, another member of staff or adult associated with school.

Electronic Devices - Searching & Deletion

In accordance to 'The Education Act 2012' school has the right to search and or delete anything from personal devices if they believe illegal or suspicious activity has taken place.

Exemptions

All the above stands unless given permission from the Head Teacher e.g. while on residential trips, permission may be given to designated staff to upload photos onto our Nether Hall School Facebook or Twitter account and for equipment to be offsite with images stored.

Review and Evaluation

This policy will be reviewed annually and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

Our Acceptable Use Policy (AUP) has been created and approved by the SLT and school governors.

This Staff Acceptable Use policy links to our:

- Child protection and safeguarding policy
 - Keeping safe online policy
 - Pupil Acceptable Use policy
 - Anti Bullying
 - Behaviour policy
 - Staff code of conduct
 - Staff disciplinary procedures
 - Data protection policy and privacy notices
 - Complaints procedure
-



Nether Hall School

Acceptable Use Policy – Staff, Governors and Volunteers Agreement

I have read, understood and agree to comply with the school Acceptable Use Policy

Signed: _____ Date: _____

Print Name: _____

Position in School: _____