`

Acceptable Use of IT

STATUTORY / NON-STATUTORY	**STATUTORY**
MEMBER OF STAFF RESPONSIBLE	DHT
DATE APPROVED BY HEAD/SLT	May 2023
TRUSTEE OR COMMITTEE RESPONSIBLE	GP
DATE OF FULL BOARD OF TRUSTEE APPROVAL	June 2023
REVISION DUE DATE	June 2025

TABLE OF CONTENTS 2
INTRODUCTION 3
AIMS 3
RELEVANT LEGISLATION AND GUIDANCE 3
DEFINITION 3
UNACCEPTABLE USE 4
Sanctions 5
STAFF (INCLUDING TRUSTEES, VOLUNTEERS, AND CONTRACTORS) 5
Access to academy ICT facilities and materials 5
Personal use 6
Remote access 6
Academy social media accounts 7
Monitoring of academy network and use of ICT facilities 7
PUPILS 7
Access to ICT facilities 7
Unacceptable use of ICT and the internet outside of the academy 7
PARENTS 8
Access to ICT facilities and materials 8
Communicating with or about the academy online 8
DATA SECURITY 8
Passwords 8
Software updates, firewalls, and anti-virus software 9
Data protection 9
Access to facilities and materials 9
Encryption 9
INTERNAL ACCESS 9
Pupils 9
Parents and visitors 10
MONITORING AND EVALUATION 10
RELATED POLICIES 10
APPENDIX A – SOCIAL MEDIA GUIDELINES 11
APPENDIX B – ACCEPTABLE USE GUIDELINES 13
Acceptable use of the internet : agreement for parents and carers 13
Acceptable use of the academy's ICT facilities and internet : agreement for pupils and parents/carers 14
Acceptable use of the academy's ICT facilities and the internet: agreement for staff, trustees, volunteers and visitors 15

Introduction

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

Aims

This policy aims to:

- Set guidelines and rules on the use of academy ICT resources for staff, pupils, parents, and trustees.
- Establish clear expectations for the way all members of the academy community engage with each other online.
- Support the academy's policy on data protection, online safety, and safeguarding.
- Prevent disruption to the academy through the misuse, or attempted misuse, of ICT systems.
- Support the academy in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our academy's ICT facilities, including trustees, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy.

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 2018
- 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
- Keeping Children Safe in Education (updated annually)
- Searching, screening and confiscation: advice for schools

Definition

The follow definitions are as follows:

- "ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- "Users": anyone authorised by the academy to use the ICT facilities, including trustees, staff, pupils, volunteers, contractors, and visitors.

- “Personal use”: any use or activity not directly related to the users’ employment, study, or purpose.
- “Authorised personnel”: employees authorised by the academy to perform systems administration and/or monitoring of the ICT facilities.
- “Materials”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

Unacceptable Use

The following is considered unacceptable use of the academy’s ICT facilities by any member of the academy community. Any breach of this policy may result in disciplinary or behaviour proceedings (see sanctions section below).

Unacceptable use of the academy’s ICT facilities includes:

- Using the academy’s ICT facilities to breach intellectual property rights or copyright.
- Using the academy’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the academy’s policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute.
- Sharing confidential information about the academy, its pupils, or other members of the academy community.
- Connecting any device to the academy’s ICT network without approval from authorised personnel.
- Setting up any software, applications, or web services on the academy’s network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the 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 academy’s ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting, or disposing of ICT equipment, systems, programs, or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the academy.
- Using websites or mechanisms to bypass the academy’s filtering mechanisms.

This is not an exhaustive list. The academy reserves the right to amend this list at any time. The Deputy Headteacher or any other relevant member of staff will use professional

judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the academy's ICT facilities.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the academy's policies, they may include revoking access to aspects of the academy IT infrastructure.

Staff (including trustees, volunteers, and contractors)

Access to academy ICT facilities and materials

The academy's Network Manager manages access to the academy's ICT facilities and materials for academy staff. That includes, but is not limited to:

- Computers, tablets, and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the academy's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Manager.

Use of phones and email

The academy provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the academy has provided.

Staff must not share their personal email addresses with parents 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 General Data Protection Regulation 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. Please see the Trusts data retention policy for further detail.

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 but must report the breach on the form in the academy's virtual leaving environment (VLE).

If staff send an email in error which contains the personal information of another person, they must inform the Network Manager / DPO immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the academy to conduct all work-related business.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

Personal use

Staff are permitted to occasionally use academy ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Network Manager may withdraw permission for it at any time or restrict access at their discretion.

Staff may not use the academy's ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the academy's ICT facilities for personal use may put personal communications within the scope of the academy's ICT monitoring activities. Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using academy ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the academy's guidelines on social media (see appendix 1) and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is always appropriate. The academy has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Remote access

We allow staff to access the academy's ICT facilities and materials remotely. This is done securely by using two factor authentication and is managed by the Network Manager.

Staff accessing the academy's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the academy's ICT facilities outside the academy.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

Academy social media accounts

The academy has several official social media accounts, managed by specific staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

Monitoring of academy network and use of ICT facilities

The academy reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Only authorised ICT staff may inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The academy monitors ICT use to:

- Obtain information related to academy business.
- Investigate compliance with academy policies, procedures, and standards.
- Ensure effective academy and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

Pupils

Access to ICT facilities

- “Computers and equipment in the academy’s ICT suite are available to pupils only under the supervision of staff”.
- “Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff”.
- “Pupils will be provided with an account linked to the academy’s virtual learning environment, which they can access from any device by using the following frog.noadswood.hants.sch.uk.

Unacceptable use of ICT and the internet outside of the academy

The academy will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following at any time (even if they are not on academy premises):

- Using ICT or the internet to breach intellectual property rights or copyright.
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the academy's policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate material.
- Activity which defames or disparages the academy, or risks bringing the academy into disrepute.
- Sharing confidential information about the academy, other pupils, or other members of the academy community.
- 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 academy's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language

Parents

Access to ICT facilities and materials

Parents do not have access to the academy's ICT facilities as a matter of course. However, parents working for, or with, the academy in an official capacity (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the academy's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the academy online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the academy through our website and social media channels.

Data security

The **academy** takes steps to protect the security of its computing resources, **data,** and user accounts. However, the **academy** cannot guarantee security. Staff, pupils, **parents,** and others who use the **academy**'s ICT facilities should always use safe computing practices.

Passwords

All users of the academy's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Software updates, firewalls, and anti-virus software

All academy ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.
Users must not circumvent or make any attempt to circumvent the administrative, physical, and technical safeguards we implement and maintain to protect personal data and the academy's ICT facilities.

Any personal devices using the academy's network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the academy's data protection policy.

Access to facilities and materials

All users of the academy's ICT facilities will have clearly defined access rights to academy systems, files, and devices.

Users should not access, or attempt to access, systems, files, or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Network Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed completely at the end of each working day.

Encryption

The academy ensures that its devices and systems have an appropriate level of encryption. Academy staff may only use personal devices to access academy data, work remotely, or take personal data (such as pupil information) out of the academy if they have been specifically authorised to do so by the Headteacher.

Internal access

The academy wireless internet connection is secure.

Pupils

Pupils may only access the Wi-Fi using their personal devices when supervised by staff using a 'temporary Wi-Fi key'.

Parents and visitors

Parents and visitors to the academy will not be permitted to use the academy's Wi-Fi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the academy in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the academy's Wi-Fi to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and Evaluation

The Deputy Headteacher and Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the academy.

This policy will be reviewed every 3 years.

Related policies

This policy should be read alongside the academy's policies on:

- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix A – Social Media Guidelines

10 rules for academy staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead.
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils.
6. Don't use social media sites during academy hours.
7. Don't make comments about your job, your colleagues, our academy, or your pupils online – once it's out there, it's out there.
8. Don't associate yourself with the academy on your profile (e.g. by setting it as your workplace, or by 'checking in' at an academy event).
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) can find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connection (such as parents or pupils).

Privacy setting

- Change the visibility of your posts and photos to 'Friends only', rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list.
- Don't forget to check your old posts and photos – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts.
- The public may still be able to see posts you've 'liked', even if your profile settings are private, because this depends on the privacy settings of the original poster.
- Google your name to see what information about you is visible to the public. Prevent search engines from indexing your profile so that people can't search for you by name – go to bit.ly/2zMdVht to find out how to do this.
- Remember that some information is always public; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if a pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile.
- Check your privacy settings again and consider changing your display name or profile picture.
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the senior leadership team or the Headteacher about what's happening.

What to do if a parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the academy.
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in.

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

What to do if you are being harassed on social media, or somebody is spreading something offensive about you

- Do not retaliate or respond in anyway.
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred.
- Report the material to Facebook or the relevant social network and ask them to remove it.
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents.
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material.
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix B – Acceptable Use Guidelines

Acceptable use of the internet : agreement for parents and carers	
Name of parent/carer: **Name of child:**	
Online channels are an important way for parents/carers to communicate with, or about, our academy. The academy uses the following channels: • Our official Facebook pages. • Email/text groups for parents (for academy announcements and information). • Our virtual learning platform. Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).	
When communicating with the academy via official communication channels, or using private/independent channels to talk about the academy, I will: • Be respectful towards members of staff, and the academy, always. • Be respectful of other parents/carers and children. • Direct any complaints or concerns through the academy's official channels, so they can be dealt with in line with the academy's complaints procedure. I will not: • Use private groups, the academy's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the academy can't improve or address issues if they aren't raised in an appropriate way. • Use private groups, the academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident. • Upload or share photos or videos on social media of any child other than my own unless I have the permission of other children's parents/carers.	
Signed:	**Date:**

Acceptable use of the academy's ICT facilities and internet : agreement for pupils and parents/carers	
Name of pupil:	
When using the academy's ICT facilities and accessing the internet in the academy, I will not: • Use them for a non-educational purpose. • Use them without a teacher being present, or without a teacher's permission. • Use them to break academy rules. • Access any inappropriate websites. • Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity). • Use chat rooms. • Open any attachments in emails, or follow any links in emails, without first checking with a teacher. • Use any inappropriate language when communicating online, including in emails. • Share my password with others or log in to the academy's network using someone else's details. • Bully other people. I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others. I will always use the academy's ICT systems and internet responsibly. I understand that the academy can discipline me if I do certain unacceptable things online, even if I'm not in academy when I do them.	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the academy's ICT systems and internet when appropriately supervised by a member of academy staff. I agree to the conditions set out above for pupils using the academy's ICT systems and internet, and for using personal electronic devices in academy, and will make sure my child understands these	
Signed (parent/carer):	**Date:**

Acceptable use of the academy's ICT facilities and the internet: agreement for staff, trustees, volunteers, and visitors	
Name of pupil:	
When using the academy's ICT facilities and accessing the internet in academy, or outside the academy on a work device, I will not: • 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 academy's reputation. • Access social networking sites or chat rooms. • 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 academy's network. • Share my password with others or log in to the academy's network using someone else's details. • Share confidential information about the academy, 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 academy.	
I understand that the academy will monitor the websites I visit and my use of the academy's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside academy, and keep all data securely stored in accordance with this policy and the academy's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager 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. I will always use the academy's ICT systems and internet responsibly and ensure that pupils in my care do so too.	
Signed (staff member/trustee/volunteer/visitor):	**Date:**