ICT and Acceptable Use Policy Statement

Date reviewed	12/01/2022
Date approved	26/01/2022
Approver	Carol Tompkins-Owen
Signature	Carol Tompkins-Owen
Next Review date	17/01/2024

Abbreviations:

DSL: Designated Safeguarding Lead
ICT: information, communication technology
LGB: Local Governing Body
PSHE: Personal, Social, Health Education
RSHE: Relationships, Sex and Health Education

Definitions

"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 school to use the ICT facilities, including governors, 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 school 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

Contents

Contents

Section 1: Introduction

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), Local Governing Board, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

Section 2: Policy Statement

This policy is an important document which governs everyone's' use of ICT at school and covers a wide range of issues surrounding the rights, responsibilities and privileges – as well as responses – connected with computer and IT use.

The policy has included input from: members of staff, representatives from the Local Governing Body, and colleagues from within Portsmouth City Council and Delta Education Trust.

Section 3: Policy Scope

This policy is for all staff, pupils, parents and carers, members of the local governing board, visitors and partner agencies working within the school.

Section 4: Policy Aims and Objectives

This policy aims to:

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

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

Breaches of this policy may be dealt with under our disciplinary policy.

Section 5: Policy Links, Legislation and Guidance

The ICT and Acceptable Use Policy Statement links to the following other policies:

- PSHE/RSHE Policy

- Safeguarding and Child Protection Policy
- Code of Professional Conduct

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
- 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

Section 6: Roles and Responsibilities

The role of the Local Governing Board:

- Holding the Headteacher and Leadership Team to account
- Monitoring the implementation of policy
- Ratifying policy
- Auditing data and measuring progress
- Being committed
- Monitoring, evaluating and reviewing

The role of the Headteacher and Leadership team:

- Provide guidance, training, policy and practice for the acceptable use of ICT
- Provide training to ensure safeguarding is central to the policy, including regular training for Cyber Security
- Record and review all training
- Provide staff with access to ICT
- Provide email and Microsoft 365 accounts to enable staff to work safely and effectively across the school

The role of teachers and support staff:

- Follow policy, practice and guidance
- Provide teaching and learning opportunities for pupils regarding IT, cyber security and social media
- Ensure pupils are safe from harm
- Understand and follow the practices as set out below:

Use work email accounts for work purposes only.

Conduct all work-related business using the email address the school has provided.

Not share personal email addresses with parents and/or pupils and must not send any work-related materials using their personal email account.

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.

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 ICT Manager and Headteacher immediately and follow our data breach procedure.

Not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business. School phones must not be used for personal matters. Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Office 365

Staff are provided with Office 365 for school work.

OneDrive enables staff to save work securely in a cloud based format. Memory sticks are not to be used.

Emails enable important information and communication to be shared. Staff are given time to read emails daily. For well-being, staff are not expected to send, read or respond to emails beyond reasonable hours.

Emails sent from the IT Manager or Director of IT from Delta Education Trust will contain vital information and must be read and directions followed.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times and not mention the school or staff by name. Staff must not search for information about pupils using personal social media accounts.

The role of parents/carers:

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school 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 school'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 school 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 school through our website and social media channels.

We ask parents to sign read and acknowledge safe internet use at induction.

The role of others:

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

- Computers, tablets, mobile phones 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 school'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 IT Manager

Requests for support must be logged using Every.

The role of PCC / Delta Education Trust

Delta Education Trust provide trust wide ICT support and management.

Section 7: Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth-produced sexual imagery)
- 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 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 school'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 school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's ICT facilities.

Section 8: Approach

8.1 Data Security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

All users of the school'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.

The IT Manager will generate passwords for pupils using a password manager/generator and keep these in a secure location in case pupils lose or forget their passwords.

In their Office 365 profile, staff will be expected to add a recent photograph for additional security.

8.2 Software updates, firewalls and anti-virus software

All of the school's 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 school's ICT facilities.

8.3 Data protection

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

GDPR-Privacy-Notice.pdf (theharbourschoolportsmouth.org)

8.4 Access to facilities and materials

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

These access rights are managed by the IT Manager.

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 IT Manager immediately.

For GDPR and data protection, users must use lock – windows key and L - to lock screen when away from their device.

Users should always log out when they have finished with a device to allow use by others.

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 down completely at the end of each working day.

Protection from Cyber Attacks

The school will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the school will verify this using a third-party audit (such as eset at least annually, to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the school needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data daily and store these backups on a cloud-based backup system. A daily back up on a virtual server will also be made.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our cloud-based provider.
- Make sure staff:
    - Enable multi-factor authentication where they can, on things like school email accounts
- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
- Have a firewall in place that is switched on and that is manged by our school's broadband.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification

- Develop, review and test an incident response plan with the IT department, for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested at least annually though ideally every 6 months and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with Delta Education Trust to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

Teaching and Learning Opportunities for Pupils

Teaching and learning opportunities for safe internet use are planned for all pupils and discussed at induction.

Safeguarding

At The Harbour School appropriate filters and monitoring systems are in place to protect pupils from potentially harmful online material including terrorist and extremist material when accessing the internet in school. The internet is a great way for children and young people to connect with others and learn new things. As interactions between people are increasingly taking place on-line it is essential that we safeguard children as robustly in the virtual world as we do in the real one.

Internet and wifi

The school wireless internet connection is secured.

Section 9: Practice and policy review process

The Harbour School's ICT and Acceptable Use Policy Statement will follow a regular review with contributions from key stakeholders.

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 rules for school 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 school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school 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) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

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

A parent adds you on social media

Staff must not respond to parental requests, decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being harassed on social media, or somebody is spreading something offensive about you

Do not retaliate or respond in any way

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 2: Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

This form will be shared at Induction and the beginning of each academic year, and recorded through a Microsoft Forms Questionnaire

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Allow pupils to access staff computers or use staff log ins – Campus SLT and IT Manager will monitor and review this
- Share my password with others or log in to the school's network using someone else's details
- Once logged into a device, allow any other uses, staff or pupil, to access the device
- 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 IT or social media in any way which could harm the school's reputation
- Access unauthorised social networking sites or chat rooms on school equipment
- Use school equipment for personal use
- Bring in personal equipment for IT use in school or working with pupils
- 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
- Unplug and alter school IT equipment installations
- Use personal technology to mirror or beam content onto classroom screens
- 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

- I understand that the school will monitor the websites I visit and my use of the school'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 school, and keep all data securely stored in accordance with this policy and the school'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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 3: ICT Equipment Agreement

IT Equipment Agreement

This Agreement defines the requirements for the safe use of all company issued devices and includes, but not limited to Cameras (including memory cards), Laptops, Mobile Handsets (phones/tablets including SIM cards, chargers and hands-free headset devices).
It is The Harbour School policy that no member of staff uses a mobile device whilst in control of any vehicle. Under no circumstance should any member of staff attempt to use the text messaging service, review/respond to emails or interact with webpages whilst in control of a vehicle. Failure to comply with this requirement may lead to disciplinary action, which may ultimately result in dismissal.

The School reserves the right to monitor the usage of any device at any time.

Individual Declaration

- I am responsible for the safe keeping of any and all devices assigned to me and will not leave them unattended at any time.

- I am not allowed to use devices outside normal working hours or at weekends unless permitted to do so by a Senior Manager. Under no circumstances am I to use devices (mobile phone) for private calls, this includes the short message service text service and data downloads for personal reasons.

- I am responsible for the security of The Harbour School information which is stored on the device and should only store the minimum amount of information necessary (to carry out any required task) which should then be deleted from the device when no longer required in line with Keeping Children Safe in Education.

- I am responsible for informing the IT Department if the device does not have up to date anti-virus protection.

- I am responsible for returning the devices to the IT Department, upon termination of employment.

- Improper use of School Devices may result in disciplinary action.

- In the event of any device being broken, lost or stolen it must be reported immediately to my SLT and the Business Manager. If it is deemed to be through my negligence, then I will be responsible for paying the full repair or replacement costs, which will be deducted directly from my salary/wages.

For the purposes of the Employment Rights Act 1996, I authorise the Company to make deductions in full or part from my salary/wages in respect of any monies owed by me to the Company as a result of my negligence or breach of Company rules.

I have received and read The Harbour School's IT Equipment Agreement and I agree to abide by the requirements therein.

Appendix 4:Glossary of cyber security terminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.

TERM	DEFINITION
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.