HOLYWELL CHURCH OF ENGLAND ACADEMY

Acceptable Use of ICT Policy

Author	MG Simpson
Responsibility	All staff and the governing body
Effective Date	September 2022
Review Date	May 2023
Approved by Business Committee	September 2022
Storage: (i) Electronic (ii) Hard Copy	(i) School network and on Google Drive / School website (ii) Policy file
Distribution	All staff and governors

1. Purpose

This is an internal policy that defines how Holywell ensures that staff understand the acceptable, and non-acceptable use of information technology assets, resources, and systems.

This policy seeks to provide guidance that promotes proper, legal and responsible use of Holywell's information technology assets.

In addition, this policy supports the school in ensuring that staff are aware of their responsibilities in using technology according to the following legislation:

- Communications Act
- Computer Misuse Act
- Computer, Copyright Software Amendment Act
- Copyright, Designs and Patents Act
- Criminal Justice and Public Order Act
- Data Protection Act
- Defamation Act
- Electronic Communications Act
- Freedom of Information Act
- General Data Protection Regulation (EU GDPR)
- Human Rights Act
- Malicious Communication Act
- Regulation of Investigatory Powers Act
- Trade Marks Act

2. Responsibilities

All users, inclusive of employees, subcontractors and suppliers with direct access to the Holywell's information technology systems are expected to conform to this policy.

Partnership Education Ltd (our IT service provider) is responsible for providing support to staff in complying with this policy.

The Headteacher is responsible for ensuring that this policy is annually reviewed and that changes are made in the event of legislation change, advice from the National Cyber Security Centre (NCSC) or compliance frameworks such as the Cyber Essentials scheme are updated.

Holywell's governing body is responsible for the review and ratification of this policy.

Our Data Protection Officers are Chris Beeden and Harriet Stringer from 'School Data Managed' - contact@school-dpo.co.uk / tel: 01234 819 820.

3. General Principles

3.1 Keeping passwords secret

All users with access to Holywell's IT systems, services and devices must keep credentials (usernames, passwords and encryption keys) secret in accordance with Holywell's Password Policy.

3.2 Locking devices when leaving unattended

All users with access to Holywell's IT systems, services and devices must 'lock' devices them when leaving the room or breaking line of sight.

3.3 Physically taking care of devices

All users with access to Holywell's IT systems, services and devices must take all reasonable precautions to prevent loss, theft or damage to them.

3.4 Not using school/trust devices for inappropriate personal use

All users with access to Holywell's IT systems, services and devices must do so without:

- Using inappropriate or offensive language, as defined within the Staff Code of Conduct.
- Bullying or intimidating others.
- Disclosing secrets or personal data in accordance with Holywell's data protection policy.
- Using them for personal entertainment, gambling or activities not related to school business without prior consent.

3.5 Not using school/trust devices to break the law

All users with access to Holywell's IT systems, services and devices must take all reasonable precautions to prevent infringement of legislation identified within the purpose of this policy.

3.6 Using IT in accordance with Safeguarding Policy

All users with access to Holywell's IT systems, services and devices must use them to support Holywell's Safeguarding Policy.

3.7 Using IT in accordance with Data Protection Policy

All users with access to Holywell's IT systems, services and devices must use them to support Holywell's Data Protection Policy.

3.8 Not avoiding technical controls designed to keep systems secure

All users with access to Holywell's IT systems, services and devices must operate them in accordance with the way in which they were designed by the vendor and the IT Service

Provider. This includes, but is not limited to, the 'rooting' or 'jailbreaking' of devices.

3.9 Not using IT systems, services or devices that haven't been approved

All users with access to Holywell's IT systems, services and devices must not use IT systems, services or devices that haven't been approved by Holywell's IT service provider and/or the headteacher. We refer to this as 'shadow IT'.

3.10 Using IT in accordance with our Cyber Security Incident Management Plan

All users with access to Holywell's IT systems, services and devices must use them to support Holywell's Cyber Security Incident Management Plan which includes reporting suspicious activity and confirmed incidents to the Headteacher and/or the Schools' Data Protection Officer (DPO).

4. Internet Access

Holywell provides internet access to all staff and students for usage relating to school business or teaching and learning.

Internet access is filtered to prevent use that does not support school business or teaching and learning. This is done to reduce the risk of the school's devices becoming infected with malicious software (malware), in addition to supporting Holywell's Safeguarding Policy.

Holywell expects all users to respect the web content filtering system, to not purposefully circumvent it, and to report any inappropriate websites to a member of staff immediately – staff should report to the Headteacher or the IT service provider; students should report to their class teacher.

Where additional credentials (such as passwords) are required specifically to access the internet, they must be kept secret and in accordance with Holywell's Password Policy.

Intentional inappropriate use may result in further restriction or removal of internet access. Severe or continuous inappropriate use may result in disciplinary action.

5. Unapproved Software

Unapproved software has not been checked for malware, authenticity, compatibility and compliance.

Software that has not already been installed on Holywell's devices is prohibited. This includes running software that doesn't require installation such as 'portable applications' that are able to be run from removable media or directly from download (for example, email attachments).

6. Bring Your Own Device (BYOD)

'BYOD' is the use of personally owned devices for work purposes. This includes mobile phones and tablets that are used for accessing any school data, including emails.

Holywell does not allow BYOD.

Personal devices are only to be used for personal use and, when connecting personally owned devices to Holywell's wireless network, they must always be connected only to the wireless network which has been segregated from critical networks. Holywell's IT service provider will first assess the device for compliance with its Information Security Policy and

provide support in connecting it to the dedicated wireless network for internet access.

BYOD devices must not be used for:

- Contacting students or their families for any reason other than in professional capacity.
- Processing (this includes storing) images and videos of students or their families.
- Processing (this includes storing) any other personal data relating to colleagues, students or their families.
- Using software that hasn't been approved by the school to process school data.

7. Data Security and Privacy

Users of IT at Holywell must always do so in accordance with Holywell's Data Protection Policy.

Removable media (such SD Cards and CDs/DVDs) are strongly discouraged and, where possible, have been prevented from being used with technical controls.

USB devices are not to be used.

Users of IT at Holywell are granted access to data only on a 'need to know' basis in accordance with Holywell's Access Control Policy.

Users of IT at Holywell have a responsibility for facilitating security updates on their devices. In practice, this means regularly restarting devices, especially when prompted to do so by the device.

Users of IT at Holywell have a responsibility for notifying the Headteacher or the School's Data Protection Officer if they suspect a breach of data security or if they suspect a breach involving personal data.

Holywell's IT service provider ensures that the school IT networks use an appropriate level of encryption. Users of IT at Holywell have a responsibility for using the encryption tools made available to them to encrypt sensitive files leaving the school's network by upload or email.

8. Unacceptable Use

Holywell's information assets should not, under any circumstances be used for the acquisition, distribution, creation, processing, or storage of:

- any form of material that can potentially be used to promote discrimination based on but not limited to disability, race, sexual orientation or gender.
- any form of material that can be used to bully, victimise, or harass others.
- unlawful material that violates intellectual property and privacy rights.
- any form of material that directly or indirectly seek to promote unlawful actions that may be threatening, extremist, or defamatory.
- any form of material that may be regarded as obscene, indecent or offensive.

User Credentials and Password security

- All issued user credentials should be kept safe and secret in accordance with Holywell's Password Policy. It is unacceptable to display passwords or store them in a location that is easily accessible, for example, writing down passwords and sticking them on a computer or desk.
- All users are required to change passwords when there is suspicion that they may have been involved in a data breach, have been notified by the Secure Schools app, have been notified by HaveIBeenPwned>> or when requested by Holywell's IT service provider.

- Unless explicitly authorised by Holywell's IT service provider, user accounts should never be shared. A user should not log into a computer system to access resources or services using another user's credentials.

Email

- The use of e-mail is an essential means of communication. In the context of school, e-mail should not be considered private.
- All users should be aware of the risks associated with using email and when handling emails.
- It is unacceptable to knowingly send or attempt to send an email with a malicious attachment or link with the intent of causing harm or disruption.
- All users should be careful to check received emails for suspicious links or attachments before clicking. All suspicious emails should be reported to the Headteacher/IT Service Provider.

Managing e-mail

The school gives all staff and governors their own e-mail account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed. All e-mails are accessed using a password. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. If necessary e-mail histories can be traced. The school e-mail account should be the account that is used for all school business.

- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- However staff access their school e-mail (whether directly, through webmail when away from the office or on non-school hardware), all the school policies apply
- Staff sending e-mails to external organisations, parents or students are advised to cc. the Headteacher, line manager or designated line manager where additional security is required.

Teachers should note: e-mails created or received as part of their school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Teachers must therefore manage their e-mail account as follows:

- Delete all e-mails of short-term value.
- The forwarding of chain e-mails is not permitted in school.
- If you are unsure of the sender of any unsolicited e-mail it should be deleted and referred to the Headteacher and/or ICT Service Provider for information.
- Staff must inform Headteacher a member of the Senior Leadership team and/or the Designated Safeguarding Lead if they receive an offensive e-mail.

Guidance on sending e-mails

- Staff must use their own school e-mail account so that they are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal purposes (inc. advertising).
- Take care when sending bulk emails – especially where 'bcc' has to be used so that recipients are not identified.

Receiving e-mails

- Staff must check their e-mail regularly (at least once daily during work hours).
- Activate the 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source; consult the network manager first.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

Replying to emails

- Do not reply 'to all' unless that is absolutely the intention. NB. The default reply mode in gmail to an email sent to groups is to 'reply to all'. Please ensure that your change this to reply to the sender directly.
- Do not copy in additional members of staff unless necessary and intended.

e-mail writing style

- Ensure messages written are professional and polite.
- Keep messages short and to the point.
- Please remember not to treat e-mail like spoken communication. e-mails often lack the signals and cues which spoken language contains, so please word emails carefully.
- Avoid using upper case for emphasis.
- Once drafted, it's a good idea to re-read the e-mail before you press 'send'

e-mailing Personal, Sensitive, Confidential or Classified Information

- Obtain express consent from your manager to provide the information by e-mail.
- Exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:
    - Verify the details, including accurate e-mail address, of any intended recipient of the information
    - Do not copy or forward the e-mail to any more recipients than is absolutely necessary
    - Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
    - Do not identify such information in the subject line of any e-mail
    - Request confirmation of safe receipt
- Use an encoded method for sending sensitive information (eg. Egress)

Internet

As previously explained, the main purpose of Holywell's internet connection is to support teaching, learning, and administrative operations, and any activity that might disrupt this is unacceptable.

- Accessing the internet for personal use or non-work-related purposes is acceptable but limited to personal time – staff must not conduct non-work-related internet searches in directed/contracted working hours – and, for student-facing staff, non-work-related use of the internet must never be used in the presence of students. All users shall be responsible for the websites they visit and the activities they conduct on the internet.
- It is unacceptable to indulge in any personal or non-work activity that consumes significant network bandwidth such as downloading very large files or live streaming.

School devices and networks

- It is unacceptable to attempt to bypass network security controls or filters.
- Where devices are shared, users should log out to prevent other users from using their credentials.

- Where the school issues a device intended to be used for remote working, only approved users should use such devices. If user-owned devices are permitted to externally access Holywell's data or services, only approved users should use this access.
- It is unacceptable to download, store, copy, distributed unlicensed material which may be subject to intellectual property and copyright laws.
- It is unacceptable to use tools that may degrade the network, scan ports, intercept network traffic, scan for vulnerabilities, reroute network traffic or alter the network configuration without approval.
- It is unacceptable to use devices in contravention of the Computer Misuse Act 1990, which makes the following an offence:
    - Unauthorised access to computer material. This refers to entering a computer system without permission (hacking).
    - Unauthorised access to computer materials with intent to commit a further crime. This refers to entering a computer system to steal data or destroy a device or network (such as planting a virus).
    - Unauthorised modification of data. This refers to modifying or deleting data, and also covers the introduction of malware or spyware onto a computer (electronic vandalism and theft of information).
    - Making, supplying or obtaining anything which can be used in computer misuse offences.

9. Monitoring

Holywell reserves the right to record and monitor the use of its IT network and facilities, subject to the Regulation of Investigatory Powers Act, for reasons including:

- Ensuring IT services and facilities remain effective and operational.
- The prevention, detection and investigation of a breach of the law, this policy or other Holywell policies, procedures or standards.
- Investigation of suspected misconduct by users (inclusive of staff and students such as plagiarism.
- Gathering information to respond to Data Subject Access Requests.
- Investigation of suspected cyber security incidents and data breaches.
- Conducting training exercises and preparing for information security incidents.

This includes, but is not limited to, monitoring (and, where appropriate, recording) of:

- Internet browsing data.
- Internet connection data.
- Communications (inclusive of email transactions and telephone calls).
- User device access and activity logs.
- User data access and activity logs.
- Bandwidth usage.

Only authorised personnel from Holywell's IT service provider may record and monitor the use of its IT network and facilities.

10. Breach of Policy

Any form of violation towards this policy may call for disciplinary measures under Holywell's staff disciplinary or Safeguarding policies.