St Padarn's Institute IT Policy

ATHROFA PADARN SANT
ST PADARN'S INSTITUTE

Document Control Table

Document Title:	**St Padarn's Institute IT Policy**
Author(s) (name, job title and organisation):	Mike Wakeman, Director of IT, Church in Wales
Version Number:	Version 4
Document Status:	Approved
Date Approved:	22 January 2024
Approved By:	St Padarn's Executive Board
Effective Date:	January 2024
Date of Next Review:	August 2024
Superseded Version	Version 3
Related Documents:	St Padarn's Research Ethics Policy The Representative Body Computer and Internet Misuse Policy and Procedure Appropriate Private Internet Use at St Padarn's, Cardiff by Formation for Licensed Ministry candidates St Padarn's Research Ethics Policy St Padarn's Disciplinary Policy The Representative Body of the Church in Wales Disciplinary Policy

Document History:

Version	Date	Author	Notes on Revisions
1	22 May 2019	Leon Hughes, Head of Communications & Technology	• First draft

2	22 March 2021	Leon Hughes, Head of Communications & Technology	• Review of policy
3	09 June 2022	Leon Hughes, Head of Communications & Technology	• Review of policy
4	30 August 2023	Mike Wakeman, Director of IT	• Review of policy

St Padarn's Institute IT Policy

1. Contents of Policy

2. Introduction

This policy is intended to provide guidelines for appropriate use of provided IT facilities. It covers the use of those facilities by staff, learners, visitors, and other persons authorised to use them. For staff this policy is in place alongside the Representative Body Computer Security and Misuse Policy 2017, it does not supersede it. The policy is subject to annual review and is subject to the approval of the St Padarn's Executive Board. Revision history of the document is available at the beginning of this document.

3. Definitions Used in this Policy

- **Core services**: The physical network, including switching, cabling, and servers.
- **Internet provision**: This includes the cabled network, firewall and gateway, and the wireless network.
- **Provided computing equipment**: This includes all equipment provided by the Church in Wales' IT Department, including mobile devices, personal computers and peripherals including display equipment.
- **Personally owned devices**: This includes any device that is owned by a user but that is used to connect to core services or to the provided internet services.
- **Users**: This includes staff, learners and anyone who has been provided with accreditation to use core services or internet provision.
- **Files**: This pertains to digital data, held on site or remotely on another Church in Wales network. It does not include manual files.

For the purposes of this document, the above will be collectively known as "IT facilities."

4. Breaches of Policy

Breach of this policy may be considered a disciplinary offence and could be dealt with under the appropriate disciplinary policy and its related procedures. Where an offence has occurred under UK law, it may also be reported to the police or other

appropriate authority. The manner in which breaches or suspected breaches shall be investigated is outlined in section 17.

5. Summary of Acceptable Use

The following applies to all use of IT facilities contained in the definitions section of this document. Some elements of this section have expanded descriptions in later sections of this document.

5.1 All use must comply with the definitions contained within this IT policy and any breaches of this policy shall be investigated in accordance with the process outlined within this document.

5.2 Users are encouraged to use the IT facilities to further the goals and objectives of their work, study, or research and to be aware that private use of the IT facilities is a privilege, not a right.

5.3 Users shall not use the IT facilities inappropriately.

5.4 The definition of inappropriate use includes all unlawful activity including use of the IT facilities for possession or retention of unlawful material.

5.5 Inappropriate use includes the following activities some of which may be unlawful in certain circumstances:

- **5.5.1** The creation, download, storage, transmission or display of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.
- **5.5.2** The creation or transmission of material, which is designed to be threatening or abusive, defamatory, invades another's privacy, creates, or maintains a hostile environment for others and/or causes other unwarranted damage or distress.
- **5.5.3** The creation, download, storage, transmission or display of material that promotes or incites racial, religious, misogynistic, or homophobic hatred, terrorist activities or hate crime, or instructional information about any illegal activities.
- **5.5.4** The creation, download, storage, or transmission of material with the intent to defraud.
- **5.5.5** The creation, download, storage, or transmission of material that infringes the copyright of another person.
- **5.5.6** Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, except where it is authorised and relates to the academic or administrative activities of the Institute and/or where that material is embedded within or is otherwise part of a service to which the user has chosen to subscribe.

5.5.7 The representation of any views and opinions held personally by the user as the views of the Institute unless the user is explicitly authorised to do so.

5.5.8 Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics or results:

- Wasting staff effort or IT facility resources
- Corrupting or destroying other user's data or violating their privacy
- Any form of denial-of-service attack
- The introduction of viruses, worms, packet-sniffing, or password detecting software
- Port scanning
- Vulnerability scanning
- Attempting to disguise the identity of the sender/origin of an electronic communication
- Unauthorised access of the network, unsecured or unattended equipment or restricted areas of the network
- Exploiting equipment compromised by malicious code
- Unauthorised use of another user's logon credentials
- Unauthorised remote access of any equipment by using, for example, Terminal Services, VNC, Telnet or SSH
- Seeking to access data, which is known, or reasonably ought to be known, to be confidential

5.6 Hardware may only be physically connected to the network if approved or issued by the IT Department.

5.7 Priority for use of Institute IT facilities shall be given to tuition and business activities over and above private use and the IT Department may reapportion network resources including bandwidth to residential areas as necessary to maintain proper functioning of the network. Action of this sort would only be taken with prior approval from Institute authorities and would be temporary in nature.

5.8 Abuse of the private use privilege includes use that:

- Interferes with the performance of Institute duties
- Interferes with any teaching or assessment event or other Institute activity
- Significantly impedes or adversely affects network performance and/or IT resources

6. Private Use of IT Facilities

IT facilities are provided solely for use by staff in accordance with their normal duties of employment, by learners in connection with their education and by occasional tutors and volunteers who contribute to programmes. All other use is private, for example by residential learners for recreational purposes.

Private use is allowed, as a privilege and not a right, but if abused will be treated as a breach of this policy.

Any information or data for private use held on IT facilities is held at the user's own risk. St Padarn's Institute does not accept any responsibility for the integrity or availability of information or data held for private use and users will not have any right of access to that information or data if they are no longer able to access the Institute's IT facilities.

All use, including private use, must comply with the "Appropriate use of Internet provision" section of this document. Any use which does not specifically breach any other section herein, but nonetheless brings the Institute into disrepute, may also be treated as a breach of this policy.

7. Compliance with UK Civil and Criminal Law

Users must comply with the provisions of any current UK law, including but not restricted to:

- The Computer Misuse Act 1990 and Police and Justice Act 2006 amendments (Part 5)
- The Copyright Design and Patents Act 1988 and amendments
- The Defamation Act 1996
- The Terrorism Act 2006
- The Regulation of Investigatory Powers Act 2000
- The General Data Protection Regulation 2018

8. Software License Compliance

Users shall comply with the terms of any licence agreement between the Church in Wales and a third party which governs the use of hardware, software, or access to data.

The Church in Wales IT Department may deploy the use of manual or automatic searches in order to ascertain compliance with software licensing as well as terms and conditions relating to software usage. Users connecting provided computing equipment in both the physical and virtual environment will be required to download software asset management software as directed by the IT Department.

9. Integrity of IT Systems

No person shall, unless directly authorised by the Director of IT, take any action which damages, restricts, or undermines the security, performance, usability, or accessibility of IT facilities. "Taking action" may include neglect, where action might reasonably have been expected as part of a user's duties. It also includes the deliberate uploading of viruses and malware, and any attempt to bypass security systems through hacking or programming.

All connections of equipment to the IT facilities must be conducted with valid network credentials, either in the form of a valid user ID or via the provision of a temporary password by St Padarn's Administrative staff. Where viruses or other potentially harmful malware are discovered, the IT Department may disconnect any physical or virtual IT system that is considered to present a risk to the integrity of the IT facilities or to the security of information within those facilities. The IT Department may deny permission to reconnect until it can be evidenced that the risk has been mitigated.

Any apparently unauthorised access, removal or modification of IT facilities must be reported as soon as practicable to the IT Department Helpdesk (helpdesk@churchinwales.org.uk) . This includes access by individuals using credentials originally issued to another person.

Users shall comply with an instruction from the Director of IT which is issued in response to a suspected, or actual breach of network security, or a reported breach of the St Padarn's IT policy**.**

The Church in Wales IT Department shall have powers to take all steps which it may deem reasonable to remove or prevent distribution of any material that is threatening the integrity of the network, to preserve information or to protect the state of the IT facilities which may include removal of access to individuals or specific devices.

10. Security and Confidentiality of Passwords

Users shall take all reasonable care to maintain the security of IT facilities and files to which they have been given access. All passwords must conform to the Group Policy assigned by the Church in Wales IT Department and must be changed as defined in that policy. Users should also be aware that the requirements of that policy will periodically change in response to a changing security landscape. Staff and learner passwords will be allocated on an individual basis by the Church in Wales IT Department. Temporary network access passwords will be assigned by St Padarn's administrative staff with the details of individuals assigned such access being recorded for monitoring purposes.

Users shall not transfer passwords, or rights to access or use IT facilities, without written consent from the Director of IT. Doing so without permission will be regarded as a breach of policy and could result in disciplinary sanction. It is the responsibility of the user to ensure the security of their passwords and any known breach of that security should be immediately communicated to the Church in Wales' IT Helpdesk. Any public notification of passwords through post-it notes, posters and the like will be regarded as a serious breach of policy, may result in disciplinary proceedings, and will be removed on discovery.

11. Appropriate Use of Internet Provision

All users may access the provided Internet services either via the physical network or through the segregated wireless network. This service is monitored as covered in section 18. The internet network is subject to filters and certain categories of website are routinely blocked. Attempts to access these websites on provided computing equipment or on privately owned devices connected to the network will be logged and reported.

Where attempted access is to material categorised as pornographic, those attempts will be reported. For staff, the report will be to the Church in Wales HR Department. For learners, the report will be to the Principal of St Padarn's Institute. Any further action will be at their respective discretion. Formation for Licensed Ministry candidates should also refer to Appropriate Private Internet Use (Section 6) at St Padarn's, Cardiff by residents for further clarification. In cases where attempts have been made to access material that is illegal under UK law, including child pornography or violent sexual imagery, the access will be regarded as a safeguarding concern and the individual may be directly reported to the Police by the Director of IT after consultation with the HR Department, Safeguarding team and/or the Principal.

As a higher education institution St Padarn's has a statutory duty to comply with the Prevent Duty and therefore attempts to access material that pertains to political extremism or terrorism will be reported in a similar way.

Attempts to access material related to gambling will be noted but will only be reported where there is a clear pattern of repeat attempts to access. This will be at the discretion of the Director of IT, but candidates should be aware that repeated accessing of gambling sites is seen as a formation issue.

12. Attempts to Bypass Internet Security

Any attempt to bypass internet filters through the use of Virtual Private Network tools, proxy servers and similar technology will be blocked and will be considered a breach of this policy. All attempts to deploy technology of this type will be logged and the user notified that their usage has been detected and that the technology is not permissible. Any repeat violations will be reported as a breach of appropriate use of internet provision and dealt with in the same way as attempts to access pornography or material pertaining to political extremism.

13. Academic Access to Inappropriate Sites

It is recognised that academics and learners will have occasional need to access content that may be blocked to conduct sanctioned research, or material which would usually be deemed inappropriate. In this case prior permission must be sought via the processes outlined in the St Padarn's Research Ethics Policy. Users can apply for temporary "whitelisting" of blocked sites to the Director of IT. The application must be supported by written confirmation by the Research Ethics Committee.

14. Peripheral Data Storage

The St Padarn's network will only allow storage devices on the network, including USB sticks, that have been approved by the IT Department and scanned prior to use. This prevents the accidental upload of viruses or malware from a corrupted device but, once approved, the device can be reused in future. It is the responsibility of the user to ensure that any sanctioned device remains free of malware or viruses and no user can pass a sanctioned device to another user. Storage devices can be used in conjunction with printers, standalone PCs and devices not directly connected to the network.

15. Software Services, Local and Cloud Storage

Enrolled learners and regular users authorised by the Director of Operations are supplied with a full Office 365 account. This provides standard office services, a St Padarn's email account and cloud storage facilities. In addition, staff will also be able to access machine local and server-based storage for their work-related information. All files stored in these locations are accessible by IT staff for the purposes of ongoing management, disaster recovery and routine maintenance. Users are strongly advised not to store personal material in these locations but, if they do so, they should store it in folders clearly marked "personal."

Staff and learners are not allowed to store material of any type that violates UK law. In addition, material of a pornographic nature will be subject to the same reporting mechanism for violations of the appropriate use of internet provision section of this document. Material that relates to political extremism or terrorism will be reported in the same way.

16. Use of Email

Staff and learners are provided with an email address. This email is solely for work use and cannot be used for private commercial activity. It should not be used as the registration address for social media accounts, online shopping facilities or any other resource likely to generate spam email activity. Staff and learners are required not to take any action that could threaten the integrity of St Padarn's Institute when using the account.

In order to maintain high standards of network security and data protection students are not permitted to automatically forward emails sent to their St Padarn's email address to a personal email address.

17. Investigation of Breaches of IT Policy

When a breach of policy has been reported or discovered, the Director of IT has the authority to suspend a user's access to IT facilities while an investigation is undertaken. The Church in Wales HR Department will be notified where such an investigation applies to a staff member. Where the subject is a learner, the Principal of St Padarn's Institute will be notified.

The Church in Wales IT Department shall have powers to access all relevant IT facilities and files and to take all steps which it may deem reasonable to remove or prevent distribution of any material which is in breach of this policy, or to preserve

information or the state of the IT facilities for the purposes of an investigation, which may include removal of any IT facilities.

As part of investigatory action, the Church in Wales IT Department reserves the right to require access to any files held on IT facilities. It may also require that any encrypted data is made available in human-readable form.

Any such investigatory action shall not prejudice any final determination of whether a breach has occurred.

18. Network Monitoring

St Padarn's Institute is required by law to bring to the attention of all users the following notices.

18.1 Regulation of Investigatory Powers Act 2000

As required by UK legislation, St Padarn's Institute draws to the attention of all users of the Institutes IT facilities the fact that their communications may be intercepted as permitted by legislation.

The legislation (including the Lawful Business Practice Regulations) provides that interceptions are authorised for:

18.1.1 Monitoring or Recording Communications:

- To establish the existence of facts, to ascertain compliance with regulatory or self-regulatory practices or procedures or to ascertain or demonstrate standards which are or ought to be achieved (quality control and training)
- In the interests of national security (in which case only certain specified public officials may make the interception)
- To prevent or detect crime
- To investigate or detect unauthorised use of telecommunication systems or
- To secure, or as an inherent part of, effective system operation

18.1.2 Monitoring received communications to determine whether they are business or personal communications.

18.1.3 Monitoring communications made to anonymous telephone helplines.

The Institute does not need to gain consent before intercepting for these purposes although we need to inform staff and learners that interceptions may take place.

18.2 General Data Protection Regulation: Monitoring

The Church in Wales IT Department hold user registration data and various information on the use of the Institute's computer systems and network; this includes log-in and log-out times, printing logs, World Wide Web cache logs and network traffic logging.

While normally only used for resolving operational problems, these logs will be analysed down to the individual user where a breach of IT policy is suspected.

The information will also be used to communicate with individuals to alert them to malfunctions within the Institute's IT facilities or to request action to correct the malfunctions which may be putting the normal operation of the IT facilities in jeopardy.

The Church in Wales IT Department may also deploy the use of manual or automatic searches in order to ascertain compliance with software licensing as well as terms and conditions relating to software usage. This may entail a search of all software programs installed on Institute IT equipment in both the physical and virtual environment. This data may be used for investigation of breaches of the St Padarn's IT policy in addition to management of the Institute's IT facilities.

In addition, statistical analysis may take place to provide management information on computer, software, printing, cache, network, and general usage for the purposes of management of the Institute's IT facilities.

18.3 Web Content Filtering

The IT Department filters web content into the Institute as it passes through the Institute's firewalls for the purpose of protecting the reputation of the Institute and to ensure that the appropriate use of the internet provision element of this policy is safeguarded.

Logging and Access: All internet activity will be logged by the IT Department and records preserved for 12 months. Logs will only be viewed in the investigation of a breach of policy. The logging system automatically flags violations of the appropriate use of internet provision as outlined in this document. The flags identify individual users and will be reported as outlined above. With this exception, high level data provided by the logs for the provisioning of metrics for management information purposes will be anonymised.

19. DarkTrace network monitoring tool

The IT Department deploy a network monitoring system called DarkTrace. This is a quasi-autonomous artificially intelligent system that passively monitors user behaviour in order to model what constitutes normal parameters of operations for each account. If those parameters are breached, for example by sending an unusually high volume of email in a short time period, the system is capable of taking actions independent of human oversight. This can include temporary locks on accounts, loss of internet access or blocks on specific webpages. This is part of general network protection and the logs produced by the system are subject to the same controls as in section 17 of this document. However, users need to be aware that the system is capable of taking independent action outside of conventional office hours. Reverting those actions requires human action and will therefore take place during the next working day.