Christ Church Cathedral Dublin

The Cathedral of the Holy Trinity
Founded c.1030

Christ Church Cathedral
Christchurch Place,
D08 TF98, Ireland

Tel +353 (01) 677 8099
welcome@christchurch.ie
christchurchcathedral.ie

Christ Church Cathedral

Acceptable Use Policy

Introduction

Information is an asset, which like other important business assets, has value to an organisation and consequently needs to be protected. This acceptable use policy covers the security and usage of all Christ Church Cathedral information and IT equipment.

Rationale

Information security protects information from a wide range of threats to ensure business continuity, minimise business damage and maximise return on investments. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it must be appropriately protected.

Purpose

This policy is intended to establish expectations for the behaviour and acceptable use of the electronic devices and user credentials that will be used to access Christ Church Cathedral secured resources. Inappropriate use exposes Christ Church Cathedral to risks such as virus attacks, compromise of network systems, services and information, reputational and legal issues.

Scope

This policy extends to current employees, volunteers, visitors, contractors and all other associated users, (referred to as ‘you’, ‘data subjects’) who operate Christ Church Cathedral licenced software and business systems. It refers to both physical and electronic information assets under the responsibility of Christ Church Cathedral. This policy should be read in conjunction with the associated supporting IT policies.

General Use & Ownership

Business Use

Christ Church Cathedral provides technology resources to support users of the systems in accomplishing the company’s business objectives. It is Christ Church Cathedral’s intent that these resources be used primarily for business purposes.

Christ Church Cathedral equipment is issued to employees with the expectation that equipment not designated as mobile will remain at its assigned office location. As such, employees may not remove company issued equipment not designated as mobile from any Christ Church Cathedral property/premises without prior documented approval from a Line Manager.

Personal Use

Christ Church Cathedral recognises that the technology resources it provides, such as e-mail and Internet access, will be used by authorised individuals for incidental personal use. Christ Church Cathedral expects that any individual using these resources do so with the discretion and sound judgment that reflects the company's values and reputation.

Ownership

All data electronically stored within any Christ Church Cathedral secured network should be considered property and wholly owned by the company. Authorised access to data processed in Christ Church Cathedral systems does not transfer ownership.

Responsibilities

The Board is responsible for setting, approving and monitoring the implementation of this policy.

Christ Church Cathedral is the data controller.

Employees

Access to Christ Church Cathedral IT systems is controlled through user IDs and passwords. All user IDs and passwords are to be uniquely assigned to named individuals and consequently, individual employees are accountable for all their actions on the IT systems.

Employees must not:

- Allow anyone else to use their user ID and password on any Christ Church Cathedral IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Christ Church Cathedral IT systems.
- Leave their password unprotected (e.g., writing it down where it can be seen by others).
- Perform any unauthorised changes to Christ Church Cathedral's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-Christ Church Cathedral authorised device to the network or IT systems.
- Store Christ Church Cathedral data on any non-authorised equipment.
- Give or transfer Christ Church Cathedral data or software to any person or organisation outside the company without the appropriate authorisation.

Employees must ensure:

- All organisation-owned laptops or devices containing company information or emails must be encrypted.
- Where appropriate, users must secure laptops that contain sensitive information by using sleep mode, cable locks or locking laptops up in drawers or cabinets.
- All users must comply with all applicable password policies and procedures.
- All monitors used for sensitive data processing must be positioned away from public view.
- Authorisation is received to install new software applications on workstations and/or mobile devices.

- All confidential information to be stored in the appropriate locations on network servers.
- Keep food and drink away from workstations to avoid accidental spills.
- Never click on document, open attachments or click on links sent by unknown senders.
- All confidential information must be appropriately saved and stored on network servers (not desktop).

Line Managers

All Christ Church Cathedral managers must ensure that their employees adhere to Christ Church Cathedral security requirements for the data and IT resources within their area of responsibility. Managers are also responsible to deny requests for unnecessary access to resources, and to request removal of access to resources when they are no longer needed by employees.

Third Parties/Contractors/Service Providers

These groups engaged by Christ Church Cathedral are to use, develop, deploy, and manage services in accordance with Christ Church Cathedral's security requirements, and to maintain auditable records demonstrating compliance. All procurement agreements with IT service providers must include descriptions of these responsibilities. Christ Church Cathedral IT services must only be used for conducting Christ Church Cathedral business or other purposes authorised by senior management. The authority to access Christ Church Cathedral information assets and use IT services must be approved by a Line Manager.

Internet and Email

All employees have a responsibility to use computer resources and the Internet in a professional, lawful and ethical manner. Use of Christ Church Cathedral internet and email is intended for business use.
Personal use of the email system should never impact the normal traffic flow of business-related e-mail. Employees are accountable for their actions on the internet and email systems.

Employees must not:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send, share or receive any data (including images, audio files) using the company network/devices, which Christ Church Cathedral considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use a work email address for any unlawful purposes to include without limitation the sending of intimate images of any person without their consent or with intent to alarm or cause distress or harm the person in the image.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Christ Church Cathedral, alter any information about it or express any opinion about Christ Church Cathedral unless specifically authorised to do so.

- Send unprotected sensitive or confidential information externally.
- Forward Christ Church Cathedral mail to personal non-Christ Church Cathedral email accounts (for example a personal Hotmail or Gmail account).
- Make official commitments through the internet or email on behalf of Christ Church Cathedral unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- Copy or remove from Christ Church Cathedral's network any company related information for personal use, either during employment or at the end of an employment contract.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval from the IT service provider (e.g., WhatsApp).
- Connect Christ Church Cathedral devices to the internet using non-standard connections or unsecured Wi-Fi (e.g., free wifi available from hotels, coffee shops, library).

Instant Messaging

Employees must demonstrate professionalism, courtesy, and good judgment when using other instant messaging tools. Some forms of instant messaging are permitted when authorised (e.g., WhatsApp. Christ Church Cathedral may amend the permitted tools list as it responds to current security threats.

Specific use of WhatsApp is permitted, however clear guidelines are in place to ensure that client details (including personal data) are only processed when and if necessary, using secure methods.

Social Media

Social media is a collective term used to describe interactive, online platforms, be they websites or apps, which allow users to upload, download and share content. Content is developed by the user.

Employees must not:

- Publish sensitive organisation-owned information on any social media platform.
- Publish any communications on a social media platform that could damage Christ Church Cathedral's interests or reputation, even indirectly.
- Engage, in any social networking: that may harm or tarnish the image, reputation and/or goodwill of Christ Church Cathedral and/or any of its employees, visitors, volunteers, suppliers or clients.
- Use social media for any unlawful purposes to include without limitation the posting of intimate images of any person without their consent or with intent to alarm or cause distress or harm to the person in the image.
- Post or misuse other employees' personal data or information, where that information has been accessed from Christ Church Cathedral without the consent of the other employee.

Clean Desk & Clear Screen

In order to reduce the risk of unauthorised access or loss of information, Christ Church Cathedral enforces a clean desk and clear screen policy as follows:

- Personal or confidential business information must be protected using available security features provided e.g., privacy screens, use of meeting rooms.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- All confidential information including client related documentation, personal identifiable information about individuals, should be placed out of sight when a work area is unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Remote Working

Where an employee accesses Christ Church Cathedral's network from a remote location (e.g., from home or elsewhere off-site) such access creates a potential weakness in the system, not least when accessed from a wireless network. As with remote access, wireless networks should be assessed on security grounds rather than solely on apparent ease of use. For this reason, the need for such access should be properly assessed and security measures reassessed before remote access is granted. Remote access will be permitted using a secure connection and will not be permitted on unsecured WIFI networks**.** For more information see Christ Church Cathedral's Remote Working Policy.

Mobile Devices

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Christ Church Cathedral's Remote Access advice detailed above and its Remote Working Policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a vehicle. It should be placed in the car boot when travelling by car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Care should be taken with the use of mobile devices such as laptops, mobile phones, and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- Mobile devices must be used by the assigned Christ Church Cathedral employee and should not be used by another employee or third party.
- Employees must ensure that they always use work mobile devices in a manner which is lawful, ethical, and efficient. Christ Church Cathedral may withdraw a mobile device from any employee who it believes is not complying with this policy or who misuses a mobile device in any manner.
- Employees must make reasonable effort to ensure that their mobile device is always secured, kept charged and switched on during working hours.
- Only software which has the correct and proper licence and has been purchased by Christ Church Cathedral can be installed and used on a mobile device. The downloading of unauthorised apps (e.g., Snapchat, Tic Toc) is forbidden.
- Employees should have their own personal mobile device if required for personal use.
- Christ Church Cathedral will include all mobile devices in an Asset Register.

Mobile Phones

Calls made from a Christ Church Cathedral mobile phone is restricted to local and national phone numbers only (i.e., calls to telephone numbers inside the Republic of Ireland). The use of mobile phones/devices to make international calls is prohibited unless authorised as needed by an employee to perform work duties such as:

- An employee is out of the country on official business.
- An employee is working off-site or out of hours and needs to contact an external service provider based abroad. When it is envisaged that a mobile phone will be required for use abroad, this should be authorised by a Line Manager. They should also ensure that when travelling abroad for work, that they are on the correct tariff.
- In case of an emergency.
- Specific requirement for the employee’s role.

Employee’s must not:

- Dial premium rate numbers from a Christ Church Cathedral mobile phone.
- Use a work phone for personal use unless authorised.
- Download communication software (e.g., WhatsApp, Viber, Signal, etc) to a work mobile device unless authorised.
- Use/hold a mobile phone while driving. The Road Traffic Act 2006 makes it an offence for a driver of a vehicle to hold a mobile phone/ device while driving the vehicle.
- Use the mobile phone for commercial purposes such as running any sort of private business.
- To transmit confidential or personal data by text, outside Christ Church Cathedral unless authorised and the data has been encrypted.
- To view, create, download, host or transmit pornographic, offensive or obscene material (i.e., information, images, video clips, audio recordings etc.), which could cause offence to others on the grounds of race, creed, gender, sexual orientation, disability, age or political beliefs.
- To retrieve, create, host, or transmit any material which is designed to cause annoyance, inconvenience, or needless anxiety to others.
- To retrieve, create, host, or transmit material which is defamatory.
- For any activity that would infringe intellectual property rights (e.g., unlicensed installation, distribution or copying of copyrighted material).
- For any activity that would compromise the privacy of others.
- For any activity that would intentionally cause disruption to the computer systems, telephone systems or networks belonging to Christ Church Cathedral.

Mobile Storage Devices

All devices must be encryption-enabled when processing sensitive or confidential data.

Software

Employees must use only software that is authorised by Christ Church Cathedral on Christ Church Cathedral’s systems. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on Christ Church Cathedral systems must be approved and installed by Christ Church Cathedral's IT service provider.

Employees must not:

- Store personal files (photos, music, video or games) on Christ Church Cathedral's IT equipment.
- Download, store and use the following applications or software without prior authorised approval:
  - WhatsApp, or other similar apps.
  - Open AI's ChatGPT, Google's BARD, Meta's LLaMA.
  - Dropbox or any other unauthorised cloud service provider.
  - Remote access software.
- Where an employee uses AI in the course of their work, the use of personal data and/or sensitive company information should not be inputted into the AI system. All scrips, reports, etc generated by AI should always be proofread for accuracy.

Viruses

Files obtained from sources external to the business, including storage devices brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services, files attached to email, and files provided by clients or suppliers, may contain dangerous computer viruses that may damage the company's computer network. Employees should never download files from the Internet, open email attachments from outsiders that are unexpected or suspicious without checking with the sender first or IT Support. (ESET anti-virus software is installed on all users' devices).

The IT service provider has implemented centralised, automated virus detection and virus software updates within Christ Church Cathedral. All PCs have antivirus software installed to detect and remove any virus automatically but if you suspect that a virus has been introduced into the network, notify the Line Manager/IT service provider immediately.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Christ Church Cathedral anti-virus software and procedure.

Bring Your Own Device (BYOD)

Acceptable use for an employee to use their own device (BYOD) at Christ Church Cathedral will be managed to ensure that access to Christ Church Cathedral resources for business purposes are performed in a safe and secure manner. The use of certain software (e.g. Outlook, Staffsavvy, Artifax) is approved for use by employees on their personal mobile device.

Christ Church Cathedral will:

- Keep a list of employees who use personal device(s) to access Christ Church Cathedral systems, or for any work-related activity.
- Maintain signed copies of BYOD agreement (see Appendix 2), ensuring that those who operate under this policy sign an agreement.
- Ensure a competent IT service provider is available to support this activity.
- Provide relevant training & guidelines in the acceptable use of Christ Church Cathedral systems.

Employees who use their own device for work related purposes will:

- Respect and adhere to this policy concerning the use of their device.
- Sign the BYOD agreement (Appendix 2).
- Check their device is registered with the IT service provider.
- Use appropriate safety measures to reduce any risks of lost/ stolen or damaged phones/ devices.
- Adhere to the same security protocols as accessing Christ Church Cathedral systems from a work-owned device.
- Ensure work related data is not accessed from a personal device that fails to meet Christ Church Cathedral’s acceptable use standards.
- Be vigilant when accessing Christ Church Cathedral systems in public and/or remote working locations so as to avoid disclosing sensitive employee/contractor or client information.

Hardware Destruction

The safe destruction of hardware containing personal data (e.g., PCs, laptops, phones, printers, scanners and fax machines) is covered by the **End-of-Life Hardware Policy**.

Copyright

Violations of the rights of Christ Church Cathedral or any person protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Christ Church Cathedral is strictly prohibited.

Unauthorised copying of copyrighted material, including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Christ Church Cathedral or the end user does not have an active license, is strictly prohibited.

Providing information about, or lists of, Christ Church Cathedral employees, its clients or suppliers to individuals or parties outside of the company is prohibited.

System Monitoring

Christ Church Cathedral reserves the right to monitor confidential company information and personal data processed on its network.

Document Reviews

This policy will be reviewed and updated annually or more frequently, if necessary, to ensure that any changes are properly reflected in the policy.

Version Control

Name of Document	Acceptable Use Policy	Last Reviewed	-
Version Number	V1	Next Review	February 2025
Date Issued	February 2024	Document Owner	HR Manager

Document History

Date	Current Version	Details of update	New Version	Completed by:

Appendix 1: List of associated IT Policies

Policy name	Purpose
Information Security Policy	This policy outlines Christ Church Cathedral's overarching approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Christ Church Cathedral's information systems.

End of Life Policy	This policy details the policy adapted to appropriately destroy physical hardware once it has reached its end of life.

Appendix 2: Bring Your Own Device (BYOD) Agreement

This Bring Your Own Device Agreement is entered into between the employee and Christ Church Cathedral.

I, ____ hereby accept that I will only use the following personal device(s) for work purposes in accordance with Christ Church Cathedral's IT Security Policies.

List personal device(s)	1.
	2.

Where I use my own device for business use, I agree to comply with the following terms and conditions.

- **Official Use**: I agree to use my personal device for authorised official business use.
- **Liability**: I understand Christ Church Cathedral is liable for all work-related charges made on this device and therefore I will ensure that I use the device responsibly.
- **Responsibility:** I will be responsible for the care and security of this device. I will ensure it has a secure PIN code/fingerprint access and is kept in a secure location.
- **Procedures**: I am aware of Christ Church Cathedral's BYOD Policy and understand the requirements for use of the device for work related purposes.
- **Leaver Procedure**: I agree to bring my device to IT so that they can delete / clear all Christ Church Cathedral related applications/software upon request or upon termination of employment.
- **Lost Device**: If my device is lost or stolen, I agree to notify my Line Manager and IT service provider as soon as I become aware of this.
- **Data Protection**: I am aware of my obligations and responsibility under data protection laws. I have read and am aware of Christ Church Cathedral's relevant data protection policies and procedures. I will operate my personal device in line with these policies.

Employee signature		**Date**	
Authorising Line Manager signature		**Date**	