CARLISLE CATHEDRAL

DIGITAL TECHNOLOGY, COMMUNICATIONS AND ACCEPTABLE USE POLICY

INTRODUCTION

This policy applies to all members of staff, including visitors. In this policy 'staff" includes employees, clergy, trustees, casual workers/workers, and volunteers (access to systems is not intended in any way to imply an employment relationship). 'Visitors' includes anyone else who comes to the Cathedral that may use our IT systems from time to time.

Acceptance of a role with the Cathedral, whether as a member of staff, volunteer, committee member or trustee, is deemed an acknowledgment that you understand and accept this policy.

CONTENTS

INTRODUCTION 1

CONTENTS 1

1. ACCEPTABLE USE 2

2. ONLINE BEHAVIOUR 2

3. USING THE IT SYSTEMS 3

4. INTERNET AND EMAIL 4

5. USING AI RESPONSIBLY 5

6. SANCTIONS AND MONITORING 5

REVIEW OF THIS POLICY 6

CARLISLE
CATHEDRAL

1. ACCEPTABLE USE

Carlisle Cathedral defines acceptable business use as activities that directly or indirectly support the business of the Cathedral.

Devices may not be used at any time to:

- store or transmit illicit materials
- store or transmit information belonging to another company
- store or transmit information belonging to the Cathedral outside its authorised systems
- harass others
- engage in outside business activities

Employees may use their mobile device to access the following company-owned resources (only with prior line management approval):

- email
- calendars
- Teams/Zoom
- Artifax
- One Drive (through the cloud only)

2. ONLINE BEHAVIOUR

The IT system is provided as a work tool to enhance delivery of service. Access to the system is provided to staff on condition that the guidelines and good practice set out in this policy are followed. As a member of the Cathedral, you should follow these principles in all of your online activities:

- Respect the privacy of others. Do not share images, contact details or other information about anybody (even if the content is not shared publicly) without obtaining their permission. Use of personal information contrary to the provisions of UK GDPR is a serious offence.
- Do not access or share materials that infringe copyright laws.
- Do not use the internet to distribute malicious software to damage, interfere with, or gain unauthorised access to the computer systems of others or carry out illegal activities.
- Ensure that your online communications and any content you share online are respectful of others and composed in a way you would wish to stand by. Any email sent can be traced and the recipient of an offensive email may take legal action against the sender.
- Do not access, create or share content that is illegal, deceptive or likely to offend other members of the Cathedral (for example, content that is obscene or offensive, promotes violence, discrimination or extremism or raises safeguarding issues). Any material which the Cathedral considers inappropriate, or offensive will be removed immediately.
- Use Artificial Intelligence (AI) wisely. AI tools, like ChatGPT and Co-Pilot, are trained on vast amounts of data to generate human like text. When you input data into these tools, it is processed on the AI provider's servers to generate a response. It's important to

understand that any data you input may be retained and used to train and improve the AI model.

All staff should access and conduct Cathedral business using the secure IT technology provided to them for their role. Users must not attempt to install any software on a Cathedral computer / laptop or run it from a peripheral memory device**.** It is the responsibility of staff with portable devices to ensure their device is regularly connected to the network, to access anti-virus systems and updates.

3. USING THE IT SYSTEMS

Whenever you use the IT systems, you should follow these principles:

- Users are responsible for the use of their account on the network and for compliance with our Social Media Acceptable Use Policy. Access to the internet including sites visited by each user is logged. Only access IT systems using your own username and password. Do not share your username or password with anyone else. Computers should only be left unattended in the locked position, or after the logging off procedure has been completed. Passwords protect the network and computer system and are your responsibility. They should not be obvious, nor should they be the same as your widely used passwords. Strong passwords must contain a minimum of 12 characters (using a three random words rather than a single word is recommended), ensuring a mix of upper- and lower-case letters, numbers and symbols (e.g. *%#$>!).
  You should not keep a list of passwords where they may be accessed and must change your password immediately if it appears to be compromised. You must not store passwords in a folder named passwords and you must not store passwords in Microsoft outlook (eg contacts section). Key members of staff / depts will store passwords in a secure site. You must not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights. In exceptional circumstances, access may be authorised by the Chief Operating Officer (COO).
- The internet and email system are filtered to stop inappropriate sites from being accessed. If, however, a web page which is offensive is accessed accidentally, it should be immediately reported by the user to their Line Manager who will take the necessary action to prevent further access to the site.
- Do not attempt to by-pass any content filters or other security measures installed on the IT systems and do not attempt to access parts of the system that you do not have permission to access.
- Do not use the IT systems in a way that breaches the principles of online behaviour set out above.
- Any property belonging to the Cathedral should be treated with respect and care and used only in accordance with training and policies provided. Laptops and other Cathedral equipment must not be left unattended in vehicles. You must report any faults or breakages without delay to the Cathedral's IT support (DAIT) and also to your Line Manager and ensure desktop computers and their surrounding areas are left clear and in good working order for the next user.

- Staff should take care when accessing the organisation's data from outside the Cathedral site/offices, in particular, being aware of surroundings, visibility of the data by nearby people and securely storing devices when not in use.
- If you suspect a cybersecurity incident, such as a lost or stolen device, phishing or malware infection, or unauthorised access to systems or cathedral data, report it immediately to the COO. The COO will investigate the incident and lead on remedial action, deal with any data protection concerns and notify the ICO if required under GDPR.

4. INTERNET AND EMAIL

The Chief Operating Officer and the Cathedral IT provider have access to all system data.

The provision of email accounts, WiFi and internet access is primarily for official Cathedral business. Unidentified email attachments should not be opened.

All emails and information contained therein is the property of the Cathedral. Staff must be aware that all information contained in emails sent or received on Cathedral systems should be routinely deleted. Emails should be kept only as long as necessary for legal, regulatory, or business purposes and in line with Carlisle Cathedrals Records Retention Schedule which is based on the Church of England Retentions Schedule as well as UK GDPR regulations. However, retained information should not be stored in emails but saved to the secure network.

Our IT service provider has set up a system that automatically deletes items held in deleted folders of Cathedral email accounts after a period of 12 months.

Staff should be alert for suspicious emails, attachments, or links, known as Phishing.

- Never provide information, click on a link, or open an attachment you are not expecting, and always verify sender details before clicking or replying.
- Report suspected phishing emails immediately to the COO and the Cathedral's IT support (DAIT). Staff should not be afraid of reporting details of suspected phishing emails.
- The Cathedral will from time to time in conjunction with (DAIT) undertake a cybersecurity training programme by sending out training emails.

Staff should be aware that internet usage may be monitored for safeguarding, conduct and performance purposes and both email accounts and web history may be accessed where necessary for a lawful purpose and with reasonable grounds – including serious misconduct, performance, wellbeing concerns, absence, extremism, potential breach of policies and the protection of others.

Where a member of staff requires access to another member of staff's email, this must be requested via email to the COO (or the Dean, in the COO's absence) and must state the reasons why.

When an individual leaves the organisation, individual email accounts will be monitored by their former Line Manager until a decision is taken to close the account. This should not normally be

for a period longer than 1 month. Important information that is necessary to be kept should be stored separately.

5. USING AI RESPONSIBLY

AI tools are an important addition to the Cathedral's IT environment and will require new skills and knowledge to use to full advantage. However, they are fundamentally IT tools like any other digital resource and as such are subject to the conditions set out in this policy

5.1 AI in Approved Software

- Cathedral systems have Co-Pilot built in as an existing AI software tool and this is the only AI tool acceptable for use. However, for safety purposes, staff should not enter any confidential data into Co-Pilot.
- The Cathedral also utilises Canva, which is a suite of AI-powered tools designed to assist users in creating designs more efficiently.
- Staff should refrain from using other AI software for work purposes, such as ChatGPT.

5.2 Safe Use of All AI

- Many of the tools available to the public will use the data shared to train large language models (LLMs) which could then present the data to other users of the tool. You must not share personal or sensitive data in AI tools.
- Check outputs before using them; AI can be inaccurate or misleading.
- Personal data must not be used on these sites.
- Any documents, material, data or analysis created entirely by or with the assistance AI must be clearly credited as AI generated.
- Internal or externally published material created with the help of AI should not be detrimental to the Cathedral and should be reviewed/approved by SMT prior to use wherever required e.g. images of the Cathedral should be real and not AI generated.

The Cathedral may from time to time provide training and awareness programs to ensure that all staff are aware of the ethical and responsible use of AI technologies. This includes supporting staff to become AI-literate.

6. SANCTIONS AND MONITORING

The COO has responsibility for ensuring that any person who may be involved with administration or investigations carried out under this policy receives regular and appropriate training to assist them with these duties.

Use of the IT resources at the Cathedral is conditional upon adherence to this policy. A breach of this policy may be dealt with as a disciplinary matter using the usual disciplinary procedures and may result in an outcome commensurate with the type and seriousness of the breach.

CARLISLE
CATHEDRAL

REVIEW OF THIS POLICY

This policy will be reviewed at least every three years and may be subject to revision. Please refer to the ALL STAFF shared area within the Cathedral's IT system to view the most recent version. If you do not have access (e.g. café staff), please ask your line manager who will provide you with the most recent version of this policy.

Reviewed by Audit and Risk Committee – September 2026
Date of next review by Head of People: 2029
Date for re-adoption by the Audit and Risk Committee: September 2029