ALL SAINTS
WOODFORD WELLS

Title	IT Acceptable Use Policy
Owner	Operations Manager
Issue Date	November 2024
Reviewed By	Bob Darby
Approved By	Risk and Governance Committee
Approved Date	March 2021 November 2024
Next Review Due	October 2025

Purpose

- To support the confidentiality, integrity and availability of information in ASWW.
- To ensure computing resources, information and information processes are consistently protected according to approved security practices, legal and regulatory requirements.
- To clearly define acceptable usage of ASWW's IT Systems, this IT Acceptable Use Policy must be followed by all users of ASWW's IT systems. No unauthorised use is permitted.
- To clearly define acceptable usage of any social network or blog

Scope

- This IT Acceptable Use Policy applies to all information stored electronically within ASWW and to all use of ASWW's computing resources.
- This IT Acceptable Use Policy applies to all IT Users: staff, interns, volunteers, consultants, and all other third parties who have authorised access to ASWW's premises and computing resources.
- ASWW monitors for compliance with the IT Acceptable Use Policy. Appropriate investigation may take place, where breaches of this policy are suspected.
- This IT Acceptable Use Policy applies to all use of social networks or blogs by staff or volunteers, during or outside of working hours.

Confidentiality

- Both during and after your work-life at ASWW's, certain information related to ASWW's operation must be treated confidentially and must not be used or disclosed unless authorised. This would include all personal information, confidential and sensitive material, and certain financial information etc.

Data Security

ASWW has legal and regulatory responsibilities that determine how they process data. They must carefully control where data is stored, who has access to it and prevent unauthorised disclosure. ASWW's IT resources - data, information and information processes - must be protected. You should ensure that:

- You only access data, equipment, software or information that you are authorised to access.
- You do not cause malicious damage of any sort.
- You always lock any device you are using, before leaving it unattended.
- You pay close attention to the physical security of devices in public places.
- You turn off your PC before leaving the premises, unless there is a valid reason to leave it on.

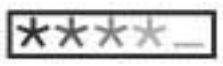
Confidential data should:

- only reside and be accessed from either ASWW servers (e.g. S Drive) or from authorised third-party systems (e.g. ChurchSuite; Trello). Authorisation for processing confidential data on third party systems is given by the Operations Manager and must be obtained in advance.
- only be copied onto a ASWW PC or laptop where there is a business reason for a local copy. However, any updated file must be uploaded onto ASWW servers or approved 3rd party system at the first opportunity.
- only be stored on your own device, where use of that device for ASWW work has been approved in advance by the Operations Manager, where there is a business reason for a local copy, and where it is "encrypted at rest"
- only be stored on a USB stick if that is encrypted

Non-confidential information may be copied onto your own device where there is a business reason so to do.

Office 365 can be used to work securely from non-ASWW equipment (see the section below, headed 'BYOD – Bring Your Own Device').

All security incidents or concerns should be promptly reported to the Operations Manager and to the IT System Administrator.



IT System Access

Logins and Passwords

A login with a Password is a unique key for accessing ASWW IT Systems. Ensure you:

- Choose strong passwords (at least eight characters with a mix of letters, numbers and other symbols) that others cannot easily guess or work out. Changing your password regularly is recommended.

- Never reveal your password to anyone or allow others to use your login and password, other than as required to the IT System Administrator as part of IT system administration and support.

Tokens (Additional Security Devices)

To access some IT Systems, you may need to use a token along with your login and password. Never share the token (or its associated PIN code), or allow other IT users to use it. Take great care to look after the token, if you mislay it then immediately report the loss to the Operations Manager and IT System Administrator.

Access from non-ASWW Premises:

Take care when accessing ASWW confidential data. Think when working outside ASWW premises e.g. using a laptop in a public place, who might possibly be able to see any data on the screen. The more sensitive the data, the more precautions around data security should be observed.

Use of email

ASWW provides email for legitimate Church communication to all ASWW employees, some contractors and those who work in the Church office. These emails have the domain "@asww.org.uk", and should be used for all church communication, rather than any other account. Other church users or groups are allowed to use their own email accounts for church related activities/ministries.

You are responsible for the content of any email you send. Care must be taken over the content of any message and must not:

- Include offensive content (including images, videos or other media), in respect to pornography, race, gender, sexual orientation, disability, age, gender reassignment, religion/belief or politics.
- Include any swearing or other unacceptable use of language.
- Constitute harassment or bullying of any sort.

Remember external email goes out bearing an ASWW email footer – the equivalent of sending a letter with a business letterhead.

When using the ASWW email system:

- As a safeguard against fraud, you should never provide your personal data via email or in response to an email.
- It's strongly recommended that sensitive or confidential data should be sent encrypted if sent external to ASWW. Remember information is not secure when sent externally unless it is encrypted.
- Take care over wording of messages as it is possible to set up a legally binding agreement by email.
- Messages may be opened in your absence, but only in exceptional circumstances.
- You are not permitted to distribute chain mail.

Occasional personal emails may be sent (and received) from your ASWW email account where they satisfy the criteria laid out in this section.

Use of the internet

The Internet, including social media sites, is a critical ASWW resource, allowing users to carry out legitimate ASWW activity more effectively. However, as an information resource it presents a business risk and needs to be used within clear guidelines. When using the internet, you should ensure that you:

- Do not access Internet Sites which contain offensive material of any sort. That is, offensive in respect to pornography, race, gender, sexual orientation, disability, age, gender reassignment, religion/belief or politics.
- Do not download or store any offensive material
- Do not access or place any material on the Internet that might be considered inappropriate, offensive or disrespectful to others.
- Do not enter sensitive data unless for a legitimate reason and the Internet site is secure, well known, has an excellent reputation and you have typed the URL into the browser.

Remember that Internet communications can be intercepted, read and misused unless encrypted i.e. using a secure site.

ASWW provides access to the Internet as a business tool - limited personal use is at your Line Manager's discretion, but such use should never affect your duties or your ability to carry out your role. You are responsible for all Internet sites accessed under your login.

Social Media

Use of blogs or social networks, such as Facebook, Twitter/X or WhatApps, has become ubiquitous and central to much business and social life. Whilst our starting point is that what people say or do outside work on these networks is private, ASWW also recognises that its reputation and people are key assets and everyone working here shares the responsibility of protecting them. If on a social media network you refer to ASWW, its work or your colleagues, or could be identified as being associated with ASWW, you should ensure that your postings do not damage the reputation of ASWW by:

- Respecting your colleagues and never publishing comments which could amount to harassment or bullying.
- Not disclosing any confidential information which relates to the ASWW business.
- Not misusing any personal data relating to your colleagues.

Generative AI (GenAI)

Use of GenAI (e.g. ChatGPT, Bard, Bing) should be ethical, comply with all applicable laws, and complement ASWW's existing information and security policies. This means:

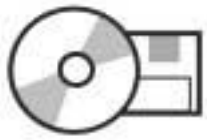
- Copyright – You must adhere to copyright laws when utilising GenAI. It is prohibited to use GenAI to generate content that infringes upon the intellectual property rights of others, including but not limited to copyrighted material
- Accuracy - All information generated by GenAI must be reviewed and edited for accuracy prior to use. You are responsible for reviewing output and are accountable for ensuring the accuracy of GenAI generated output before use/release.
- Confidentiality - Confidential and personal information must not be entered into a GenAI tool, as information may enter the public domain. Users must follow all applicable data privacy laws and ASWW policies when using GenAI.

  Ethical Use - GenAI must be used ethically and in compliance with all applicable legislation, regulations and ASWW policies. Users must not use GenAI to generate content that is discriminatory, offensive, or inappropriate.

Virus and spyware prevention

Computer viruses, spyware and malware can disrupt and damage ASWW's IT systems and business. This means:

- Viruses, Spyware and malware must be prevented from gaining access to ASWW's IT Systems. Do not maliciously allow viruses, spyware or malware onto ASWW IT Systems.
- Software, documents, discs and external recording materials (e.g. usb memory sticks) may carry viruses or spyware. Internet downloads can also introduce viruses and spyware onto IT systems. Take care over what is accessed on ASWW IT Systems - using trusted sources minimises risk to ASWW.
- Do not tamper with the anti-virus or any other security software installed on a ASWW device.



Software

It is the legal obligation of ASWW and its employees to comply with copyright laws and respect the intellectual property rights of others. You are not permitted to:

- Use unlicensed or illegal software or computer files
- Possess, use, reproduce or distribute software on any ASWW computer without authorisation.

Only software approved by the Operations Manager is permitted to be loaded onto ASWW equipment or downloaded from the Internet. Software and software licenses may only be purchased or obtained through requests to the Operations Manager.

Procurement

All IT hardware, software and telecommunications equipment, other than BYD (see below), must be procured through the Operations Manager's office and pre-approved by the IT Systems Administrator. This includes but is not limited to PCs, laptops, tablets, printers, scanners, and software or applications.

Disposal of computer equipment and media

When PCs, laptops or any other devices holding data are no longer required or are to be replaced, they must be returned to the IT Systems Administrator office to be decommissioned. Under no circumstances should computer equipment be given away or dumped as data can be obtained from disks not decommissioned correctly. If this procedure is not followed, information sensitive to ASWW could become available to unauthorised individuals and cause a breach of the Data Protection Act.

Data Protection

ASWW has to comply with the Data Protection Act 2018 and the General Data Protection Regulation (EU) 2016/679. The Act applies to any information which relates to identifiable, living individuals and to whatever medium is used to record the data e.g. paper, computer or CCTV. For all information held on computers ASWW has to notify the Office of the Information Commissioner: stating reasons for doing so; who is having information held on them; the types of information being held, and to whom the information can be disclosed. This notification must be completed before information can be held. ASWW also has to provide a Data Privacy Notice that informs people how we collect, process and use their personal data.

There are further obligations on the part of anyone who wants to process personal data. Do not process personal data unless you understand and apply the eight good data handling principles, as detailed in the Data Protection Act.

BYOD – Bring Your Own Device

We recognise that many staff at All Saints' have to use personal computers / mobile devices to perform the duties associated with their role at All Saints'. To ensure the user's personal device and the All Saints' data on your device(s) are kept safe you should:

- Recognise that the physical security of the device(s) is your responsibility, and always take appropriate steps to keep your device(s) secure
- Ensure the device is protected from unauthorised use by a password or PIN code
- Install an industry standard virus protection system/app and keep it up to date
- Take great care when opening emails from unknown sources. Ensure all attachments are scanned before being opened
- Report any security incidents (such as virus infections) promptly to the Operations Manager and to the IT System Administrator.
- Ensure all confidential data is only stored and accessed through Office 365 or any other system explicitly approved by the Operations Manager.

Your acceptance of ASWW's IT Acceptable Use Policy

All users of ASWW IT Systems are required to accept the IT code of practice.

Breaches of ASWW's IT Acceptable Use Policy

We would consider each breach of the IT Acceptable Use Policy carefully and individually. We would prefer to resolve any issue arising out of such a breach informally. However, if the matter was sufficiently serious action will be considered under the staff Disciplinary Procedures. Where the breach is by a volunteer, the PCC may decide to remove that volunteer from involvement in the relevant activity. If the breach constitutes a posting on a social media network which breaches this IT policy, ASWW may also ask you to remove the content.