# FUW GROUP
# INFORMATION HANDLING POLICY

**Overview**

The purpose of this policy is to ensure that all staff understand how information in their care should be protected, communicated and shared with other parties and their responsibilities to manage information assets in order to protect against the consequences of breaches of confidentiality, loss of integrity, interruption to availability and non-compliance with legislation which would otherwise occur.

This Information Handling Policy has been based on the principles of GDPR. The FUW Group as an organisation is committed to following IT best practices in terms of permissions, granting access, monitoring and retaining data. In addition to IT best practices in terms of information handling, the Group is also committed to electronic security best practices. It is essential for all company employees and users of our IT systems to understand and follow company policies.

**Scope**

This policy applies to all the FUW Group employees, consultants, contractors, and temporary workers both onsite and offsite, including all personnel affiliated with third parties engaged by the Group. This policy applies to all IT equipment that is owned or leased by the FUW Group.

This policy is a non-contractual document and is subject to change. The most recent copy will always be made available on the company Intranet, or directly from the FUW Group's IT Department on request.

## 1. General Principles:

1.1. All company data must be treated as confidential, employees must only access customer information as a function of their role and necessary to carry out their duty.

1.2. Every digital document and email created and stored within the Group's Google Workspace email/data system, constitutes an organisational record; no messages contained within it are considered personal.

1.3. Staff are granted access to email and the internet for the Group's business use and for work related educational and research purposes.

1.4. The FUW Group control, provide and manage the company's information technology network services and control all staff access to the internet and email under instruction of the Group's Head of IT and the IT support company.

1.5. Be aware of the information you are sharing. Ensure that the information is relevant to the recipient, especially if the email is addressed to more than one person.

1.6. Be professional in all your communications.

1.7. Report any incident/breaches where you have accidentally responded to or clicked a link in a phishing email. Report it to both the Head of IT and the IT support company.

## 2. Emails

Email accounts and their contents are owned by the FUW Group, however individual users are accountable for the contents of emails sent from the Group's email accounts.

1.1. The Group's business must be conducted strictly through the company's email system. Personal email accounts must not be used for work. The Group's emails are monitored and stored on the cloud for reasons that are legal and comply with GDPR. All company's emails are retained, this includes deleted email messages.

1.2. Confidential documents must only be sent by a secure means of transfer. If sending confidential documents via email, they must be password protected. If sending password protected documents by email, passwords can be transmitted by voice call, text message, or a separate email message that does not reference the original document. Another possibly easier and faster way would be to ask the IT Technical team's helpdesk to send confidential documents on your behalf.

1.3. The language used in emails must be professional in terms of content and tone at all times.

1.4. Care must be taken when addressing email messages. They must be sent to the intended recipient and this includes when forwarding, replying and copying other company users or other external recipients into the message. Misaddressing official company communication is considered a data breach and must be reported immediately to your line manager.

1.5. Long chain email messages should be avoided to have better control on the addressees and the context of the information being communicated.

1.6. When communicating by email, be mindful as they have the same status as any other form of business correspondence or written communication and may be subject to disclosure under a Freedom of Information request and subject to Data Protection Legislation.

1.7. It is strictly forbidden to setup automatic email forwarding from any of the FUW.org.uk email accounts, to any external and/or personal email account outside our Group, e.g., name.lastname@fuw.org.uk forwarding to name.lastname@yahoo.com.

1.8. The decision of email forwarding and to revoke email forwarding during colleagues' absence, must be under the responsibility of the employee's line manager who needs to send the request by email directly to the external technical support team.

## 3. Google Workspace system – Google Drive

3.1. Users must be extremely careful when sharing documents, folders or Shared Drives internally and externally. This is to ensure that only the intended person or persons has/have access to the document(s). Sharing documents with an unintended person or persons is considered a confidentiality breach of GDPR and needs to be reported immediately to the line manager.

3.2. Documents within Google Drive must not be shared by the use of “anyone with the link” because it is impossible to control access via this type of link, which can be passed on to and accessed by unauthorised users as there are no restrictions attached to it. Also, the link can be published or posted anywhere on Internet.

3.3. Company employees and users must not share any work documents with their personal Google account or other cloud service account.

3.4. All documents created by the Group’s employees are considered the intellectual property of the organisation. They must always be saved within the company’s Google Workspace system in Google drive, because it provides encryption and is backed up every day. Files are never to be saved on:

a. Any personal electronic devices.

b. Locally on any company device or anywhere within the Remote Desktop Environment, such as in “Documents” on a Windows computer, on any external storage device, (e.g., USB flash drive/stick).

## 4. Voice control systems and spoken confidentiality

4.1. Spoken confidentiality must be done in appropriate places where there is no risk of being overheard and away from active Voice Control Systems.

4.2. When working from home you must make sure you are not overheard by visitors.

4.3. When working from home you must turn off any form of Voice Control Systems such as Alexa, Google, Cortana, to avoid possible eaves-dropping from the voice activated assistant on personal devices such as: Alexa, Google, Cortana (as part of Windows).

## 5. Confidential Physical documents

A confidential physical document is any physical document that contains any information about a client or sensitive information about the company. This includes any paper document, printed or handwritten.

5.1. Care must be taken when handling or carrying confidential physical documents. They must not be left unattended. They should be stored in a locked cabinet or drawer when not in use.

5.2. Care must be taken when addressing physical documents to be sent via post or courier. They must be sent to the correct intended recipient.

5.3. The destruction of confidential documents must be done using shredders and collected together for confidential waste disposal. Non-confidential paper waste should be recycled.

5.4. Think before you print to minimise environment's impact and the financial costs involved.

**Policy Violation and the Consequences of Policy Violation**

Information handling is crucial to the running of the business and failure to follow this policy could result in detriment to the company, staff and/or clients and may lead to a breach of data and possible infringement of UK and EU law. GDPR breaches must be reported and investigated which may lead to company fines, loss of reputation and loss of revenue. Company employees that are negligent in terms of the principles of this policy may face disciplinary action and/or dismissal.