[Company]

INFORMATION

TRANSFER POLICY

Transferring Information

1 Document Version Control

	Last Modified	Last Modified By	Document Changes
0.1	[DATE]		Document first created

2 Document Contents Page

3 Information Transfer Policy

3.1 Purpose

The purpose of this policy is ensuring that correct treatment when transferring information internally and externally to the company and to protect the transfer of information using all types of communication facilities.

3.2 Scope

All employees and third-party users.

Information that forms part of systems and applications deemed in scope by the ISO 27001 scope statement.

3.3 Principles

Data transfer must comply with all legal and regulation legislation requirements including but not limited to the GDPR and Data Protection Act 2018.

Formal agreements that include non-disclosure and confidentially clauses must be in place for data sharing prior to the data transfer.

Personal data must not be transferred outside the European Economic Area without legal consent, justification, and legal mechanisms in place.

No personal or confidential information is to be transferred unencrypted.

All transfers are in line with the Information Classification and Handling Policy

3.4 Information Virus Checking

Information that is transferred is virus checked before being sent or before being opened when received.

3.5 Information Encryption

Personal and confidential information is always encrypted before being transferred.

Encryption credentials for username and password where used are shared via two separate and distinct communication methods. The preferred method is to share the username via email and the password via a voice call.

3.6 Data Transfer Methods

3.6.1 Preferred Transfer Method

The preferred transfer method is (- describe how we transfer data based on DropBox, Sharefile, Google Drive, One Drive, Company portal).

3.6.2 Data Transfer by Email

Email is never the best solution for transferring information as it is not secure and is not a guaranteed delivery mechanism.

Consideration is always given to an alternative secure method of transferring sensitive data wherever possible and practicable.

Email communication should not be used to transfer unencrypted personal or confidential information.

Email messages must contain clear instructions of the recipient's responsibilities and instructions on what to do if they are not the correct recipient.

Care must be taken as to what information is placed in the subject line of the email or in the accompanying message. Filename or subject line must not reveal the full contents of attachments or disclose any sensitive personal data.

The use of a personal email account is not permitted.

3.6.3 Data transfers by post/courier

Data transfers which occur via physical media such as paper reports, memory cards or CDs must only be dispatched via the company approved secure courier with a record of collection and a signature obtained upon delivery. The use of Royal Mail first class, second class, special delivery or recorded delivery is not permitted.

The recipient should be clearly stated on the parcel and the physical media must be securely packaged so that it does not break or crack.

The recipient should be advised in advance that the information is being sent so that they are aware when to expect the information. The recipient must confirm safe receipt

as soon as the information arrives. The sender responsible for sending the data is responsible for confirming the data has arrived safely.

3.6.4 Data transfers on removable media / memory sticks

Only company owned removable media is to be used for transferring information in line with policy the device usage is approved, recorded in the asset register, assigned, and encrypted.

The removable media must be returned to the owner on completion of the transfer and the transferred data must be securely erased from the storage device after use. The asset register must be updated.

Clear instructions of the recipient's responsibilities and instructions on what to do if they are not the intended recipient must be given.

Any accompanying message or filename must not reveal the contents of the media.

The process described for **Data transfers by post / courier** must be followed.

3.6.5 Telephones, Mobile Phones and General Conversations

As phone calls may be monitored, overheard, or intercepted (either deliberately or accidentally), care must be taken as follows:

- Be conscious of your surroundings especially on public transport such as trains and public places such as coffee shops when discussing personal, confidential, or otherwise sensitive information.

- Personal data must not be transferred or discussed over the telephone unless you have confirmed the identity and authorisation of the recipient.
- When using answer phones do not leave sensitive or confidential messages or include any personal data. Only provide a means of contact and wait for the recipient to speak to you personally.
- When listening to answer phone messages left for yourself, ensure you do not play them in open plan areas which risks others overhearing. Delete them immediately after listening.

3.6.6 Data Transfers over Bluetooth

Bluetooth is not approved as a communication method for unencrypted confidential, personal, or otherwise sensitive data.

- Ensure device mutual authentication is performed for all accesses.
- Enable encryption for all broadcast transmissions (Encryption Mode 3).
- Configure encryption key sizes to the maximum allowable.
- Establish a —minimum key size for any key negotiation process. Keys should be at least 128 bits long
- For Bluetooth: Use application-level (on top of the Bluetooth stack) authentication and encryption for sensitive data communication such as SSL.
- Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages.

- Note: A “secure area” is defined as a non-public area that is indoors away from windows in locations with physical access controls.
- Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the users ‘s devices.
- Use only Security Mode 3 and 4. Modes 1 and 2 should not be allowed. Security Mode 3 is preferred but v.2.1 devices cannot use Security Mode 3.
- Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, or images.
- All Bluetooth profiles except for Serial Port Profile should be always disabled, and the user should not be able to enable them.

3.7 Lost or missing information

If it is discovered or suspected that information has been lost, is missing, did not arrive, or has gone to the wrong person then the employee or external party user is required to inform at least one of their line manager, the information security management team, the management review team, or the senior management team immediately at which point the company Incident Management Process will be followed.

4 Policy Compliance

4.1 Compliance Measurement

The information security management team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

4.2 Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

4.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.4 Continual Improvement

The policy is updated and reviewed as part of the continual improvement process.