INFORMATION EXCHANGE POLICY

Policy Statement

Information is an asset that like other business assets must be adequately protected. This principle is especially important when Organisational information is exchanged with external third parties such as third party suppliers or clients.

This Policy is designed to ensure that when Organisational information is sent externally from the business it is done so in a safe and secure manner and that the information exchange process is auditable, robust and is compliant with all legal and regulatory requirements.

Scope

The scope of this Policy applies to:

1. All confidential information assets including, but not limited to, client data, corporate data and employee data
2. The external transfer of confidential information via any electronic medium, e.g. e-mail, FTP or Website
3. The external transfer of any physical copies of confidential information, e.g. Courier or Royal Mail
4. All Organisation staff, contractors, temporary staff and external third party suppliers who exchange/receive Organisational information.

Objectives

The objective of this policy is to establish a controlled environment that ensures:

1. The Organisation's information exchange procedures are secured from unauthorised access, modification or theft
2. Exchange agreements or contracts are in place that covers responsibilities and liabilities between the Organisation and external third parties
3. Users are aware of their responsibilities when sending Organisational information to a third party supplier or a client
4. Incident management procedures are in place should any Organisational information be lost or stolen whilst being sent to an external third party
5. The Organisation's information exchange procedures comply with all legal and regulatory matters.

Principles
General Principles:

1. Loss of data or any other incident suspected of impacting the secure external delivery of the Organisation's confidential information should be reported to the Organisation's Information Security Manager or the IT Helpdesk as soon as possible.
2. Incident management procedures should be established to ensure that any reported loss or theft of either electronic or physical data whilst in transit is appropriately managed.

3. Retention and disposal procedures should be established within exchange agreements or contracts to ensure data exchanged is disposed of in a secure and timely fashion and is in accordance with all legal and regulatory matters.

4. Liabilities for secure information exchange and secure processing of this information must be agreed and documented through contracts with the third parties prior to any exchange taking place.

5. Where a third party will store, process or retain any confidential Organisational data, a review of the third party's Information Security standards must be carried out before the transfer occurs.

Classification Scheme

The Organisation has an Information Classification scheme in place that allows staff to identify information that must be encrypted when being sent out of the business. The details are as follows:

1. **Confidential** – Includes information such as advice we give to a client, minutes of client meetings, client's strategy documentation, client finances or client personal employee or member details (up to and including name, address, NI, bank details) or equivalent internal information

2. **Restricted** – Includes business plans, company strategy and associated papers, employee details, internal policies, processes and procedures, legal advice or the firm's financial data

3. **Internal** – Includes information such as internal memos, ongoing project information or minutes of internal meetings

4. **Public** – Includes information such as marketing brochures, client or company details or other information already available in the public domain.

Electronic Data Exchange

1. All electronic external data transfers involving confidential or restricted information must be secured using industry-standard encryption techniques. The Organisation's corporate e-mail encryption solution is one such standard. Note: Password protecting a document such as Word, Excel or PowerPoint does not always provide sufficient protection.

2. Where confidential or restricted electronic data is sent via hardware, e.g. CD-ROM, USB device or tape drive, the device itself must be encrypted. The device must also be sent by approved courier.

3. Passwords used to encrypt the information must be a minimum of 8 characters in length and must be alphanumerical in nature and must contain at least one special character e.g. ! % * $.

4. Passwords used to secure the information must be sent under a separate cover, e.g. by telephone and only divulged to the pre-agreed recipient of the information.

5. Procedures must be in place to confirm successful delivery or otherwise.

6. Unprotected confidential or restricted electronic information must never be sent over a public medium, such as the Internet.

7. Where appropriate, digital signatures should be used to ensure non-repudiation of electronic data transfers.

8. E-mailing confidential information to a web based e-mail system such as Yahoo or Hotmail is strictly prohibited, even if using the corporate e-mail encryption solution.

Physical Data Exchange

1. Where physical copies of confidential or restricted information are sent to an external third party, these must only be sent by an approved method or delivered by hand by an Organisation employee.
2. Where an employee is carrying confidential or restricted information outside of the office environment, they must ensure the data is properly protected and carried at all times by the employee.
3. Physical copies of confidential data including CD-ROM's must only be sent by approved courier or by Royal Mail recorded delivery. Where a Courier or Royal Mail Recorded Signed-For service is used, the process must be secured by the following principles:
    - Only use authorised couriers from a preferred supplier list
    - Use couriers who can track the data from pick up to destination
    - Verifying the identity of couriers on pick up
    - Obtaining proof of posting
    - Where large packages are being sent the use of tamper-free packaging
    - Delivery of package must be to a prearranged singular point of contact
    - Recording of a signature on delivery to recipient
    - Online confirmation of delivery via Track and Trace service.

Responsibility for implementation

Internal IT Manager

Revision

This Policy will be reviewed as per the date below.

/olicy Sign-off

Date of Issue:	27/10/2020
Date of Next Review:	15/09/2021
Name:	Tim Barber
Signed:	

Amendment History

Version	Modified On	Modified By	Comments
1.0	15/09/2020	Jo Holloway	
2.0	27/10/2020	Jo Holloway	Updating dates