

P10 Information Exchange Policy

1 Policy Statement

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

This Policy is designed to ensure that when TCHC 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.

2 Scope

The scope of this Policy applies to:

- All confidential information assets including, but not limited to, client data, corporate data, and employee data
- The external transfer of confidential information via any electronic medium, e.g. e-mail, File Transfer Protocol (FTP) or Website
- The external transfer of any physical copies of confidential information, e.g. Courier or Royal Mail
- All TCHC staff, contractors, temporary staff, and external third-party suppliers who exchange/receive TCHC information.

3 Objectives

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

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

4 Principles

General Principles:

- Loss of data or any other incident suspected of impacting the secure external delivery of TCHC confidential information should be reported to TCHC Head of IT, IT Department and Managing Director (MD) as soon as possible if the MD is unavailable a Director must be notified.
- 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.
- 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.



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

5 Classification Scheme

TCHC has an Information Classification scheme in place that allows staff to identify information that must be encrypted when being sent out of the business. See the P81 Data Protection Policy. The details are as follows:

Restricted

Includes highly sensitive business data such as financial data, intellectual property, business plans, company strategy and all other key operational information. This also includes customer/learner/employee personal data as specified by UK GDPR. This information must be encrypted before being sent outside of the organisation and should only be shared with authorised personnel.

Confidential

Includes contracts, reviews, disciplinarys and any other sensitive information that should only be accessible to the parties directly involved. This information must be encrypted if sent outside of the organisation and care must be taken to ensure it is only sent to the relevant personnel, if shared internally it must be done so through secure channels such as a restricted access SharePoint site or a OneDrive link with access set only the specified personnel.

Internal

This information should not be shared outside of the business and includes any data that is only relevant for the Organisations employees, such as internal memos, internal policies and procedures, ongoing project information, internal meeting minutes, organisation charts and internal processes. Should a need arise for any such internal information to be shared externally it must be approved by your line manager and information of a sensitive nature must be encrypted prior to transmission. When these files are shared internally, rather than password protecting individual files employees should utilise the SharePoint workspaces for collaborative working on documents.

Public

Includes information such as marketing brochures, general company details or other information already available in the public domain. There is no need to encrypt this data before transit.

6 Electronic Data Exchange

All electronic external data transfers involving client or confidential information must be secured using industry standard encryption techniques. TCHC 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 which is why you must follow TCHC's procedures on how to encrypt documents.

Where confidential 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.

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



Passwords used to secure the information must be sent via a separate channel of communication, e.g. by telephone and only divulged to the pre-agreed recipient of the encrypted information.

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

Unprotected confidential or customer/learner electronic information must never be sent over public medium such as the Internet, if information is to be shared over the internet then it must be protected.

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

7 Physical Data Exchange

Where physical copies of confidential information are sent to an external third party, these must only be sent by a company approved method or delivered by hand by a TCHC employee.

Where an employee or associate is carrying confidential information outside of the office environment, they must ensure the data is properly protected and with them at all times.

Physical copies of confidential data including CD-ROM's, Hard Drives or USB drives must only be sent by a TCHC employee or associate, approved courier or by Royal Mail recorded delivery. Where a Courier or Royal Mail Recorded Sign For service is used, the process must be secured by the following principles:

- Only use authorised couriers
- 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 signature on delivery to recipient
- Online confirmation of delivery via Track and Trace service.

8 Revision

This Policy will be reviewed at least annually.



Claire Jeens
Quality Director - TCHC GROUP LTD

Document History

Reference No	Version	Date	Author	Classification	Review Date
P10	1.0	12/11/2020	Claire Jeens Alex Irvine	Unclassified	12/11/2021



P10	1.1	07/06/21	Alex Irvine Claire Jeens	Unclassified	07/06/2022
P10	1.2	26/05/2022	Alex Irvine Claire Jeens	Unclassified	26/05/2023