P81 Data Protection & GDPR Policy

1 Introduction

The purpose of this document is to define the TCHC Group Data Protection Policy.

The TCHC Group is committed to ensuring its compliance with the requirements of the General Data Protection Regulation (GDPR). We recognise the importance of personal data to our business and the importance of respecting the privacy rights of individuals.

A failure to comply with this policy could expose the business to enforcement action by the Information Commissioner Officer (ICO) or to complaints or claims for compensation from affected individuals. This could have a severely adverse impact upon the TCHC Group.

We treat breach of confidentiality as a serious matter. Anyone found to be in breach of confidentiality, or any sensitive data will be liable for disciplinary action as laid on the in the Company Handbook.

This document forms part of your conditions of employment for employees. All employees must read the policy completely and confirm that they understand the contents of the policy and agree to abide by it. All employees must follow our Data Protection Policy and the Data Protection Act and if they breach the Policy or Data Protection Act, they will be investigated, and this may result in disciplinary action. A separate Data Sharing Agreement is available for all TCHC Group Sub-Contractors, Partners and Suppliers to complete and sign.

Data is considered a primary asset and as such must be protected in a manner commensurate to its value. Data protection is necessary because data processing represents a concentration of valuable assets in the form of information, equipment, and personnel. Dependence on information systems creates a unique vulnerability for our organisation and the employee. Security and privacy must focus on controlling unauthorised access to data. Security compromises or privacy violations could jeopardise our ability to provide service; lose revenue through fraud or destruction of proprietary or confidential data; violate business contracts, trade secrets, and customer privacy; or reduce credibility and reputation with its customers, shareholders, individuals and partners.

The main objective of this policy is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorised or inappropriate access, use, modification, disclosure, or destruction. This policy applies to all of our data and all customer data assets that exist, in any of our processing environments. The processing environment is considered to be, collectively, all applications, systems, and networks that we own or operate or that are operated by our vendors.

This policy defines the TCHC Group's overall security and risk control objectives that we endorse. The premise for the policy can be stated as: "Other than data defined as public, which is accessible to all identified and authenticated users, all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorised entities." This embodies the principle of least privilege where everyone starts with access to nothing and is given access on a need must basis.

1.1 Scope of the Policy

This policy applies to all TCHC Group and customer data assets that exist in any TCHC Group processing environment, on any media during any part if its life cycle. The following entities or users are covered by this policy:

Full or part-time employees of TCHC Group who have access to TCHC Group or customer data. TCHC Group vendors or processors who have access to TCHC Group or customer data.

Other persons, entities, or organisations that have access to TCHC Group or customer data.

Another purpose of the policy is to protect the information assets[1], (see notes below), of TCHC GROUP from all threats, whether internal or external, deliberate or accidental.

It is the policy of TCHC GROUP to ensure that:

- Information will be protected against unauthorised access. Confidentiality of information will be assured[2].
- Integrity of information will be maintained[3].
- Regulatory and legislative requirements will be met[4].
- Business Continuity plans will be produced, maintained and tested[5]. Information security training will be available to all staff.

All breaches of information security, actual or suspected, will be reported to, and investigated by the Data Protection Officer.

Business requirements for the availability of information and information systems will be met.

The role and responsibility for managing information security, referred to as the Information Security Manager, will be performed by the Data Protection Officer.[6]

All Team Leaders and Managers are directly responsible for implementing the policy within their areas of responsibility, and for adherence by their staff and associates.

It is the responsibility of each employee and associate to adhere to the policy.

Notes

1. Information takes many forms and includes data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes and diskettes, or spoken in conversations and over the telephone.
2. The protection of valuable or sensitive information from unauthorised disclosure or intelligible interruption.
3. Safeguarding the accuracy and completeness of information by protecting against unauthorised modification.
4. This applies to record keeping and most controls will already be in place; it includes the requirements of legislation such as the Companies Act and the Data Protection Act.
5. This will ensure that information and vital services are available to users when they need them.
6. This may be a part or full-time role for the allocated person.

1.2 Breach of Policy and Enforcement

It is the responsibility of all our employees, associated staff, suppliers, partners, sub-contractors, employers, participants, learners, third-party vendors and hosts to assist us to comply with this policy. A breach of this policy could have severe consequences to employees, TCHC Group, and the person or company involved. This may cause consequences for the ability to provide services, or maintain the integrity, confidentiality, or availability of services. Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action. Severe, deliberate, or repeated breaches of the policy may be considered grounds for gross

misconduct; or in the case of a TCHC Group vendor, termination of their contracted services. All those listed above are bound by these policies and are responsible for their strict enforcement.

1.3 UK General Data Protection Regulation (GDPR)

The UK General Data Protection Regulation (GDPR) is a European Union "Regulation" which serves to protect the personal data of anyone in the UK. The term "Regulation" means that once the GDPR was published in January 2021, it instantly became law in the UK. This differs from an EU "Directive" which each country interprets into its own law. A regulation is implemented verbatim, ensuring a level of consistency across all EU members.

From May 2016, the GDPR entered into a two-year transition period, giving organisations time to understand the new regulation and ensure compliance. This meant that on May 25th, 2018, GDPR was enforced and must be complied with from this date. Following on from Brexit, the new UK GDPR was published on the 1st of January 2021 and became law on this date. The spirit of GDPR focuses on protecting the individual, not applying controls onto companies.

The UK GDPR builds on the 1995 European Data Protection Directive, which each EU country interpreted into its own data protection laws, e.g. the UK 1998 Data Protection Act. These country specific laws are now mostly superseded by the UK GDPR, creating a harmonisation of laws across the continent.

Whilst the content of the UK GDPR is extensive, there are a number of key highlights:

1. **Enhanced Rights** – The Data Subject has greater rights than before, with direct control over the usage, retention and movement of personal data. This includes the right to erasure, also known as the right, to be forgotten, and also the right to portability. The notion of portability allows data subjects to access their personal data that controllers are holding, and have it sent to another controller. Rights to consent are now much tighter, with controllers generally needing to provide greater detail of what processing is to be performed along with unambiguous opt-in style consent. Additionally, opting out and removing consent should be made very simple. The Data Subject is now much more in charge of their data.
2. **Fines and Penalties** – If you fail to comply with the GDPR then the costs can be huge. The maximum "administrative" fine that a regulator can impose is £17.5 million or 4% of annual turnover of the parent company. These fines are purposefully high in order to be "effective, proportionate and dissuasive." Additionally, data subjects themselves and collective groups have the right to take Controllers to court and sue for damages. In many large breaches, a class action lawsuit would be more costly to the controller than any administrative fines from the regulator.
3. **Breach Notifications** – If a data controller has a breach of personal data, depending on the severity of it they have 72 hours (from the point of detection) in which to notify the regulator and potentially the affected data subject.
4. **Data Processors in Scope** – Previously, Data Processors (e.g. a cloud hosting provider, or email delivery company) were not in scope for many of the data protection requirements. Instead, all the responsibility for a failure came down to the controller. The GDPR changes that, and now Processors share the burden of data protection.
5. **Data Protection Officers** (DPO) – Organisations that process large amounts of data or special categories of data (sensitive data) or are Government entities will need to designate a DPO. This person is the organisation's Data Protection lead and the principal advisor in all data protection activities.

Our Data Protection Procedure for IT is as follows:

Enforcing password changes every 60-90 days which is enforced via technical controls.

Encryption of all mobile devices capable of storing large quantities of data (Laptops, smart phones, USB drive, etc.)

Making sure all electronic devices capable of accessing information are password protected or encrypted.

Ensuring access to systems and data is set based on a combination of least privilege and role based access, so individuals by default have the minimum amount of access required for their job role.

All electronic equipment and information assets are logged, recorded and monitored.

No administrative rights are granted to any user on any system with the exception of the IT team.

Any device that is disposed of or that requires data destruction is subject to permanent deletion of such information by formatting or destruction of Hard Drive or any data storage devices. Logs of equipment and data destruction are maintained by the IT Department.

All electronic devices will require active and up-to-date virus protection and the latest system security patches.

1.4 Data Protection Officer (DPO)

The DPO assists the TCHC Group in maintaining data protection compliance. The DPO offers expert advice, supports data protection impact assessments and audits and act as the intermediary between data subjects, the organisation's business units and the supervisory authority. The DPO will investigate, take ownership and report as required with recommendations in the event of a data breach and will have deep understanding of the organisation's data protection.

The DPO's contact details are publicly available for data subjects to access and employees know who the DPO's are and how to engage with them.

Data Protection Officer – Claire Jeens – **dataprotection@tchc.net**

Day to day, the DPO is the internal authority on data protection guidance for all activities involving personal data. Any new project, architecture, design or plan that includes personal data has the input from the DPO. In turn, availability of the DPO for all teams is essential. The DPO's guidance does not necessarily need to be followed, but if it is not, then this should be explicitly documented as to why and the risk assessment made. The DPO sits in an area of the business where there isn't a conflict of interest and has a direct line of communication into the TCHC Board.

The DPO, is NOT responsible or accountable for Data Protection compliance. This duty falls on the organisation, employees and individuals.

Reporting process

If you discover a breach of GDPR you should report this straight away using the company reporting document to the Data Protection team via e-mail to **dataprotection@tchc.net**.

Types of breaches are

- Sending an e-mail with a CV containing personal information sent without encryption
- Sending an e-mail containing someone's financial information which the person can be identified form such as national insurance number and date of birth without encryption
- Providing personal learner information to an external party such as their name, signature, and unique learner number who did not need to have it for any purpose.

2 Data Life Cycle

The security of data can be understood through the use of a data life cycle.

The typical life cycle of data is:

1. Data usage
2. Data transmission
3. Data storage
4. Data retention and destruction

The following sections provide guidance as to the application of this policy through the different life cycle phases of data.

2.1 Data Usage

All users that access TCHC Group or customer data for use must do so only in conformance to this policy. Uniquely identified, authenticated and authorised users must only access data. Each user must ensure that TCHC Group data assets under their direction or control are properly labelled and safeguarded according to their sensitivity, proprietary nature, and criticality. Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

Users of data assets are personally responsible for complying with this policy. All users will be held accountable for the accuracy, integrity, and confidentiality of the information to which they have access. Data must only be used in a manner consistent with this policy.

2.2 Data Transmission

All users that access TCHC Group or customer data to enable its transmission must do so only in conformance to this policy. Where necessary and when required, data transmitted must be secured via encryption mechanisms. This may include the use of confidentiality and/or integrity mechanisms.

2.3 Data Storage

All users that are responsible for the secure storage of TCHC Group or customer data must do so only in conformance to this policy. Where necessary, data stored must be secured via encryption mechanisms. This may include the use of confidentiality and/or integrity mechanisms. Access control mechanisms must also be utilised to ensure that only authorised users can access data to which they have been granted explicit access rights.

2.4 Data Retention and Destruction

TCHC Group only stores data for the length of time required by contract. The retained data is archived, and access is removed unless required by the contract holder.

Retention Schedule

Record	Statutory Retention Period	Authority
Accounting	Private companies – 3 years; Public companies – 6 years	s. 388 Companies Act 2006
Income Tax, NI returns, HMRC correspondence	3 years after the end of the financial year	The Income Tax (Employments) Regulations 1993

Children/young adults	Until the child reaches 21	Limitation Act 1980
Retirement Benefits Schemes	6 years from the end of the scheme year	The Retirement Benefits Schemes (Information Powers) Regulations 1995
Statutory Maternity Pay (calculations, certificates, medical evidence)	3 years after the end on the tax year in which the period ends	The Statutory Maternity Pay (General) Regulations 1986
Wage/salary (overtime, bonuses, expenses)	6 years	Taxes Management Act 1970
NMW	3 years after the end of the consequent pay reference period	National Minimum Wage Act 1998
Working time	2 years after they are made	The Working Time Regulations 1998
ESF Training provision All projects under the ESF 2014-2020 programme	10 years after the final ESF claim is paid by the ESF Managing Authority.	UK GDPR and Data Protection Act 2018 ESF Managing Authority

Record	**Recommended Retention Period**
Application forms and interview notes	6 months to a year
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Permanently
Inland Revenue/HMRC approvals	Permanently
Money purchase details	6 years after transfer or value taken
Parental leave	Until child is 18 (birth/adoption)

Pension scheme investment policies	12 years from the ending of any benefit payable under the policy
Pensioners' records	12 years after end of benefit
Personnel files, training records (disciplinary records, working time records)	6 years after end of employment
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years after date of redundancy
Statutory Sick Pay records, calculations, certificates, self-certificates	at least 3 months after the end of the period of sick leave, but 6 years after the employment ceases advisable
Time cards	2 years after audit
Trade Union agreements	10 years after end
Works Council minutes	Permanently
First Aid, Accident Reporting and Near miss	3 years from the date of incident

Destruction of Paper-based Data

When paper-based documents that contain sensitive or confidential information have been marked for or requested for destruction they must immediately be placed in the shredder box. When the shredder box is nearing its maximum capacity the Office/Centre/Finance Manager will call 'Shred on Site' an industry approved shredding company to pick up the shredder box to remove and shred the contents on site. This must be witnessed and recorded by HR who will receive the invoice as proof that the contents were destroyed.

Confirmation is sought from the Managing Authority, prior to the destruction of any paper-based documents in relation to ESF projects.

Electronic Data

When electronic data that contains sensitive or confidential information have been marked for or requested for destruction, the IT team will use robust methods to ensure data is erased effectively.

When part of or the whole contents of a Hard Drive or other storage media needs to have its data removed a request is made to the IT Department who will locate the data, back up and archive if required and then mark it for deletion using specialist software. TCHC then use self-contained industry approved programme software which securely wipes parts of or whole hard disks and other storage media devices.

The physical destruction of data media such as physically destroying a Hard Drive or CD ROM is carried out by our IT Department by physically drilling several times into the storage media such as the hard drive platters or the CD ROM. This renders them unusable.

Logs are kept of all data destruction.

When a data subject requests their personal data to be removed, TCHC will locate all known data records of that data subject and remove all personal data from the record unless required to keep it for contractual reasons. The data subject will be informed when their data has been removed or our reasons for needing to keep it. A record of all requests and actions on data removal is kept.

Confirmation is sought from the Managing Authority, prior to the destruction of any electronic data in relation to ESF projects.

3 Data Controls

3.1 Data Ownership

To classify data, it is necessary that an owner be identified for all data assets. The owner of data is responsible for classifying their data according to the classification schema noted in this policy. If an owner cannot be determined for a TCHC Group data asset, the DPO must act as its custodian. Claire Jeens (Quality Director) is the designated person who the Data Protection Officer reports to on behalf of the Data Controller.

The default classification for all data not classified by its owner must be either confidential customer data or Proprietary company data. The DPO is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

3.2 Data Content

The nature of specific data content that exists in the processing environment, and the controls that should apply to these, is dependent upon various factors. This policy does not mandate or endorse particular data content. Rather, the business decision process used to evaluate the inclusion or exclusion of particular data content should consider those items listed below. Regardless as to the specific data content that exists in the environment, all aspects of this policy must be enforced. Considerations for evaluating data content include:

- Legal and regulatory obligations in the locales in which we operate.
- Can privacy, confidentiality, security, and integrity of the data be ensured to the satisfaction of customers and legal authorities?
- Do customers require or demand access to specific data content.
- What is common local practice?
- What rules govern the movement across international boundaries of different data content, and do we have in place controls to enforce these rules?

3.3 Data Classification

Data classification is necessary to enable the allocation of resources to the protection of data assets, as well as determining the potential loss or damage from the corruption, loss or disclosure of data. To ensure the security and integrity of all data the default data classification for any data asset is either Confidential Customer Data or Proprietary Company Data. The Data Protection Officer is responsible for evaluating the data classification schema and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavours, to develop additional data classifications. 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. 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, disciplinaries 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.

3.4 Data Encryption

Please refer to P13 – Crytpograhic controls Policy.

What is Encryption?

Encryption is the process of converting information using an algorithm to make the information unreadable to anyone except those possessing the decryption key required.

TCHC GROUP wishes to ensure that its electronically held data is adequately protected from loss and inappropriate access, whether by theft or accident. In addition, the GDPR requires TCHC GROUP to have in place appropriate policies and procedures which provide for the efficient and safe storage of data covered by the Regulation at all times.

To reduce the risk of unauthorised access, TCHC GROUP has established a comprehensive policy of encrypting data which covers data which is stored on:

- Laptops
- E-mails
- Cloud
- Computers
- Handheld devices such as Smart Phones and Tablets

- Portable storage devices e.g. memory sticks, external drives Removable media e.g. CDs or DVDs, backup tapes

Encryption standards

TCHC GROUP has determined that all data stored on portable equipment should be encrypted using a minimum of AES 256-bit encryption. Software and systems to support this have been and continue to be implemented comprehensively.

The security of TCHC GROUP data is the responsibility of every individual working for TCHC GROUP it is incumbent upon the individuals to understand their responsibilities to protect data at all times and to use encryption tools and services to achieve this.

The use of personal equipment to store TCHC GROUP data is strictly prohibited as it is unlikely that the necessary safeguards are in place to protect TCHC GROUP data in line with national guidance.

Implementation

By default, encryption will be applied to all laptops, so that any data saved will automatically be encrypted. Users will not be asked for specific passwords for individual documents or groups of documents unless they form part of specific departmental work areas.

For portable storage devices, such as memory sticks, where they must be used encrypted devices will be supplied. These will be encrypted using individual passwords so that their portability is maintained. The use of non-encrypted storage devices is prohibited for all types of data storage.

For removable media such as writeable and readable CDs and DVDs encryption will be applied by prompting the user for a password.

Handheld devices including Smart Phones and Tablets will be encrypted using the built in Content Protection facility.

If a handheld device cannot be encrypted:

- It must not be used to store customer/person identifiable data
- It must not be connected to any other TCHC GROUP system, whether by a physical (for example, Ethernet, USB or Firewire cable) or wireless connection (for example infra-red, Bluetooth or 'WiFi')
- Devices which cannot be encrypted should not be used. If possible and cost-effective, any such devices should be replaced.

Password management

In general, the password for a device or storage medium allows data to be decrypted. Passwords must be kept confidential and follow the guidelines defined in section 3.7 Passwords.

In addition, if the device is used to transfer information, the password must be sent separately by text message or verbally so that only the intended recipient has the ability to decrypt the data.

Responsibilities

Staff and Contractors who are permitted to use removable devices in the performance of their duties must ensure the data is encrypted in accordance with TCHC GROUP guidance.

The IT Manager is responsible for ensuring that TCHC GROUP has appropriate data encryption capabilities in order to protect data that is processed.

The IT Officers are responsible for assuring that the data encryption functionality and procedures used by TCHC GROUP have been implemented correctly and are of appropriate strength and fit for purpose.

Line Managers are responsible for the day to day management of their staff to ensure policies and procedures are being implemented appropriately.

Monitoring Compliance

Distribution and maintenance of encryption software will be managed by the IT Support Department Non-compliant devices may be detected and disabled using management systems installed for this purpose without notice.

Regular monitoring checks will be undertaken to ensure compliance with the criteria set out above All incidents or problems must be reported to IT Support.

Loss of Customer/Personal Identifiable Data is deemed a serious incident and must be reported by the DPO to the Information Commissioner's Office (ICO) in accordance with the GDPR. This must be reported within 72 hours of the breach being identified.

3.5 Data Back Up

Please refer to the P02 Backup Policy.

TCHC data stored locally on in-house servers and remotely on cloud servers are backed up automatically when you save a document to secure and encrypted servers. All data backups are logged, and date stamped in order to enable data restore if required through any accidental erasure of data.

3.6 Access Control

Please refer to the P08 Access Control Policy.

Responsibilities

All staff are responsible for ensuring that this Policy is complied with.

Overall responsibility for the security of the Organisation's networks rests with the Board of Directors who may delegate day-to-day technical issues regarding access control.

The Head of IT is responsible for the day-to-day technical issues and ensuring that TCHC GROUP has access control to be compliant.

All of the Organisation's employees are responsible for controlling access to any information in accordance with this Policy at all times.

Network Access

Access to the Organisation's network and cloud is controlled by means of individual user logins and passwords.

Immediately on receiving a log-in and password, the user will be forced to change the password to one that they have created in accordance with the organisations Password Policy. Thereafter, the operating system will automatically prompt for a password change at maximum intervals of 60 days or as determined by the Head of IT.

Access to accounting and operations software is controlled by means of log-in and password. This information is given only to users who need to work with the respective packages, and their level of access is controlled by permissions allocated to the various log-in identities.

Logins and passwords are not to be revealed to anyone, even a colleague, supervisor or manager. Users may access the network and their own files by logging on to the system. However, access to network objects is limited by individual logins that are authorised on the basis of operational requirements.

User rights are decided by the Programme Managers and Directors and are not to be changed without authority. These rights are reviewed at regular intervals.

User rights are kept to the minimum necessary for efficient working. Anyone who feels that they would work more efficiently with increased user rights must justify this to their line manager.

Users must not allow other users to access any systems via their log-in, either by logging in deliberately on the other's behalf or by logging in and leaving the PC unattended.

Monitoring is implemented on all systems to record log-in attempts and failures, successful logins and all changes made.

Anyone who suspects there may have been a breach of network access rules must report it immediately to IT.

Access to online information

Information stored on the servers and in the cloud can be if authorisation is permitted made available to all users, to certain defined users, or to the creator only. This is determined by the application of suitable access rights.

Sensitive information that is kept on the network are to be protected by the removal of all access permissions from any non-approved user.

Should a hacker gain access to the network, every obstacle that stands in their way will offer some protection to sensitive data. Therefore, directories and documents containing such data are not to be named in such a way as to make them easily identifiable. Names indicating Confidential, Top Secret etc. are not to be used.

Access to paper-based information

Sensitive information on paper, such as personal or financial data, is accessible only to authorised persons.

Access must be controlled by means of storing in locked cabinets. Sensitive information is not to be left lying on desks overnight. The individual must take responsibility to report to their line manager if there is no storage available. Line managers must ensure that individuals are storing all documents appropriately.

All wastepaper containing sensitive business information is to be shredded.

Further measures to prevent unauthorised access to information

Apart from the measures outlined above, access to the Organisation's premises, information systems and information is further limited by the following general instructions:

No employee who is entrusted with a password is to reveal or share this with a fellow employee or external visitor. All staff must avoid leaving laptops/PCs unattended and logged-on. Devices must always be shut down, logged off or a password-protected screensaver to be activated before walking away from the machine. All staff must use the Cloud when working with and saving company documents.

In the case of equipment destined for repair or disposal, information stored on hard disk or other storage media is to be protected as follows:

- Any hard disk intended for repair or contained in equipment being sent away for repair is fully backed up or cloned before dispatch.
- If the disk contains sensitive information, the Directories or files containing the information are removed before dispatch.
- Any storage media containing data/information, including USBs, hard disks, floppy disks, tape cartridges, CD disks etc. that are faulty or no longer required are rendered unreadable before disposal.
- Disposal of computer equipment is the responsibility of the Head of IT and with the approval of the Managing Director and is to be carried out by a reputable specialist disposal firm and disposal records are kept for both Information Security and Environmental reasons.

Data should not be transmitted or shared outside of the Organisation unless it is for business use. Should data be required to be sent or transmitted from the Organisation's premises then information stored on hard disk or any other medium is to be protected by the following means:

- No computer equipment is to leave the Organisation's premises unless specific permission has been obtained.
- Transportation of data is only undertaken by reputable carriers or by the Organisation's employees.
- the Organisation's employees who are transporting computer equipment or storage media take precautions to protect such items from theft as may be required by the Organisation's insurers.
- All data transferred to memory devices must be considered for encryption in accordance with the instructions of the client.
- Any company equipment that is authorised to be taken home must be in a locked car boot in transit and in a cupboard at home when not in use.

When employees leave the Organisation, the following action is taken:

- The employee's access rights to all IT systems are revoked
- The relevant e-mail account is disabled
- Employees are required to reveal all Passwords they may have used to protect documents or files created or processed in the course of their duties
- Employees are required to return any keys swipe cards or other security devices entrusted to them, plus any credit cards, laptops, mobile phones, printers, digital voice recorders, chargers, resources and training manuals
- The responsibility for arranging these measures lies with the Line Manager handing over to the IT Manager where appropriate

General

Although the organisation has taken reasonable technical and material precautions to prevent unauthorised access to its information systems, every individual employee can make a decisive contribution to the Organisation's security. Access control of all kinds depends to a great extent on employee's active participation, watchfulness and consistent compliance with the spirit of this Policy.

3.7 Passwords

Please refer to the P01 Password Policy.

This clause sets out the rules, requirements and guidelines covering the management of Passwords on the Organisation's IT systems. Passwords are important because they provide entry to the Organisation's IT resources, access to the network, e-mail, business applications etc. Passwords play an important role in the defence against malicious misuse of these resources. Any misuse of Passwords could result in the

confidentiality, integrity or availability of vital information being compromised or in the organisation being held responsible for illegal activities such as transmittal of offensive material via its communications systems.

Responsibilities

All of the Organisation's Staff are responsible for ensuring that this Policy is complied with.

All of the Organisation's employees are responsible for maintaining Password security in accordance with this Policy in all of their activities carried out on behalf of the Organisation.

Any employee who has temporary or permanent knowledge or use of a Password relating to any part of the IT system for which they do not normally have access, should identify this to the IT Manager immediately, so that the situation can be rectified. Any deliberate or negligent breach of this rule has a high probability of being regarded as gross misconduct and may result in immediate dismissal in which case the Managing Director will be notified.

Password Management

In general, there are three levels of Password protection: Network Access, Application Access and Document Access.

Login names for access to the Organisation's own network are supplied by the IT Department with a default Password that is to be changed immediately. The staff are prompted to change their Passwords at intervals to be determined by the Head of IT.

Access to business applications is by means of login ID's and Passwords. The level of access, or permission level, is determined by the supplied login. Employees may be required to change to a new Password when instructed by the IT Manager.

Password Creation

The objective is to create a Password that will withstand attempts to 'crack' it, at least for a reasonable length of time. For example, any word in the dictionary can be cracked within seconds by widely available Password breaking programs, whereas a well-constructed Password can take a day or more to crack and should deter all but the most determined hackers.

Passwords are to be created using the following rules:

- Passwords must be 8 characters or greater.
- Characters should be a mix from some or all of the following groups to form a medium to Strong password:
  - English uppercase characters (A...Z)
  - English lowercase characters (a…z) Base 10 digits (0…9)
  - Non-alphanumeric characters selected from the following: "$%^&*()-_=+[]{};:'@#~,<.>/?\| (Do not use £, € or a SPACE).
  - Passwords must not contain all or part of the user's name or job function, or any term (like a birthday, a partner's name or a street address) that could be easily guessed or researched.
  - Simple substitutions (such as 1 for i, 0 for O, 5 for s etc.) in recognisable words – i.e. words found in a dictionary – afford no real protection and must not be relied on.
  - Similarly, commonly used or easy to guess combinations or series such as 1234abcd, A5DFghJK, $taRwaRr$, 1passw*d etc. must not be used.

Passwords will be forced to be changed, at the discretion of the Managing Director, if the MD is unavailable then a member of The Board of Directors should be contacted. If an individual needs to access a colleague's email or documents. Where line managers need to gain access to their staff's emails or documents that they must ask the IT Manager.

Password Precautions

Please refer to our P01 Password Policy.

4 Data Sharing Agreement

It is the responsibility of the Programme Manager or Supply Chain Manager to ensure that all new and existing sub-contractor, suppliers and partners have a Data Sharing Agreement with TCHC. The onboarding and yearly due diligence checks, (those listed above), must ensure those who work with and process personal data as part of their contract with TCHC have a data sharing agreement in place.

5 Data Consent/Privacy Statements

Access to TCHC's Data Consent and Privacy Statement must be made available to all customers on relevant paperwork and through our online systems and websites.

Where consent is being requested then it must be by an 'opt in' approach. Each consent must be recorded against customer records with the data only being used for the purpose in which it was intended.

5.1 Right to Portability

Article 20 of the GDPR provides the right of data portability. That is, if TCHC has data related to a person, then that person is allowed access to it.

Portability is about providing the data to the data subject and anyone else they choose, in a format that they can understand and that someone else can import automatically.

Data Subjects can request a copy of the personal data held on them, for free. (We can now only charge for these requests if we can demonstrate they are vexatious, overly repetitive or overtly costly.)

The Data has to be provided in a format that the requestor can easily understand and that another controller could easily import, e.g. list of emails as separate email files rather than one big pdf document, or a contact list in csv file.

TCHC must send the data to a third-party controller (e.g. competitor) if requested to do so by the data subject "without hindrance".

TCHC should offer different tools for data portability, e.g. direct download tools for the data subject and automated transfer tools for transmitting the data to another controller.

TCHC is not responsible for protecting the data that has been received by the data subject or a third-party controller.

The right cannot infringe others' rights, e.g. providing someone else's personal data that touches ours.

Data and information must only be ported where authorised by the line manager in agreement with the DPO. It must only be used for business use whilst employed or providing services for TCHC.

Scope

Only personal data is in scope for a portability request. Any data that is anonymous or doesn't concern the subject is not in scope. Pseudonymised data is in scope.

The right applies to data "provided by the data subject", as opposed to "inferred data" and "derived data" which are data generated by the service provider such as algorithmic results.

5.2 Right to Erasure

TCHC have exceptions to rights to erasure included in the exceptions section below. TCHC collect personal data for the purposes of government funded contracts that:

- Comply with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority

TCHC will follow the data protection legislation outlined by the data controller for how personal information will be processed. See the privacy notice for more information:

https://www.gov.uk/government/publications/esfa-privacy-notice/education-and-skills-funding-agency-privacy-notice-may-2018

Where personal information is captured that is not a requirement for the data controller TCHC may become the data controller.

Article 17 of the GDPR, The Right to Erasure, states:

Data Subjects have the right to obtain erasure from the data controller (TCHC), without undue delay, if one of the following applies:

1. TCHC doesn't need the data anymore
2. The subject withdraws consent for the processing with which they previously agreed to (and TCHC doesn't need to legally keep it)
3. The subject uses their right to object (Article 21) to the data processing
4. TCHC and/or its processor is processing the data unlawfully
5. There is a legal requirement for the data to be erased
6. The data subject was a child at the time of collection

If TCHC makes the data public, then we are obligated to take reasonable steps to get other processors to erase the data.

Exceptions

Data might not have to be erased if any of the following apply:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation
- For the performance of a task carried out in the public interest or in the exercise of official authority
- For archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
- For the establishment, exercise or defence of legal claims

Out of Scope

Non-electronic documents which are not (to be) filed, (i.e. data you cannot search for), e.g. a random piece of microfiche, or a paper notepad, are not classed as personal data in the GDPR and are therefore not subject to the right to erasure.

6 Penetration Testing

TCHC carries out annual penetration testing on all its in-house servers and ports as well as our cloud platform. The testing assesses the strength of our protection systems from unauthorised access using a number of top-level tools and methods to gain access. A full report is produced highlighting where there might be any holes or breach in our systems so we can quickly and effectively correct.

7 Data Protection Impact Assessment (DPIA)

TCHC carry out Data Protection Impact Assessments (DPIA) which identifies and records how personal data may be used by any particular project, programme and contract and that the TCHC Group engage with. It is a device to assess risk and to also justify why and how we use data for any one particular project, programme and contract. The DPIA document is reviewed and updated annually for each project, programme and contract.

8 Data Audit

TCHC carries out a full data audit annually to review how it keeps data and to check its compliance against the GDPR. The data audit covers all electronic and paper-based systems of recording and accessing data. An analysis report produces the Risk Assessment which the DPO manages in order to reduce risks.

9 Employees of the TCHC Group

As an employee of the TCHC Group, we collect and store personal and sensitive data as a condition of employment. We only collect data that is purposeful for employment in order, for example, to process wages, expenses, references, tax information. We keep this data during the whole of your employment with the TCHC Group. You may request edits to this data to reflect changes in circumstances. You may, at any time during your employment, request a copy of all the data we hold about you.

You hereby consent to the TCHC Group processing your personal Data for any administrative or security function required by, or in order to maintain, the TCHC Group's legitimate business interests, including, but not limited to, processing systems, global communications, telephone recording, contingency planning, security of systems and premises (CCTV, card entry systems, IT security systems), systems development and testing, monitoring Internet, email and telephone usage and any other such activities as notified to you in any security policy issued by the TCHC Group from time to time.

You are entitled to request access to any personal data concerning you which is held by the TCHC Group. If you wish to do so, you should make a written request to HR. This will be provided for free unless the request is deemed to be 'manifestly unfounded or excessive'. TCHC Group will aim to provide you with the information within One calendar month of the request. There may, however, be circumstances in which the TCHC Group cannot release information to you, for example, where it contains the personal data about another employee or third party.

You shall ensure that when your personal details change, you shall inform HR in writing as soon as is reasonably possible, providing all updated personal details in order for the TCHC Group to maintain the accuracy of the Employee's Personal Data. In particular, you must inform HR immediately in writing of any change to:

- Your home address or personal telephone numbers, personal e-mail address (even for a temporary period).
- Your marital status.
- Your legal change of name.
- Your nationality or citizenship status.
- Your visa or work permit status.
- Your bank/building society account details.
- Your next of kin and their contact details.
- Any criminal convictions

Once you leave employment from the TCHC Group, we will retain your information in line with current legislations. Please see the retention table in this policy. We keep information for this period should you request a reference from us or if the HMRC require any further information for us to process your tax records. When this period has elapsed then all your data will be removed from the TCHC Group systems.

I certify that this is a true copy of the original document:

Signed

Date

Position in organisation

Name of organisation

Claire Jeens
Quality Director - TCHC GROUP LTD

Document History

Reference No	Version	Date	Author	Classification	Review Date
P81	1.1-3	01/05/2018	Mark Williams	Unclassified	01/05/2020
P81	1.4	29/07/2020	Claire Jeens	Unclassified	29/07/2021
P81	1.5	29/01/2021	Kim Kitchener	Unclassified	29/01/2022
P81	1.6	21/05/2021	Kim Kitchener Claire Jeens	Unclassified	21/05/2022
P81	1.7	05/07/2021	Kim Kitchener	Unclassified	05/07/2022
P81	1.8	16/07/2021	Kim Kitchener	Unclassified	16/07/2022
P81	1.9	05/04/2022	Kim Kitchener Claire Jeens	Unclassified	05/04/2023
P81	2.0	02/08/2022	Claire Jeens Alex Irvine	Unclassified	02/08/2023