Data Protection Policy

Index

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.

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. 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 in today's environment 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 organization. Security and privacy must focus on controlling unauthorized access to data. Security compromises or privacy violations could jeopardize 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 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 unauthorized 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 authorized entities." This embodies the principle of least privilege.

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 organizations that have access to TCHC Group or customer data.

1.2 Breach of Policy and Enforcement

It is the responsibility of all of our employees, associated staff, suppliers and third party vendors to assist us to comply with this policy. A breach of this policy could have severe consequences to the TCHC Group, its 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 instant dismissal; or in the case of a TCHC Group vendor, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

1.3 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a European Union "Regulation" which serves to protect the personal data of anyone in the EU. The term "Regulation" means that once the GDPR was published in May 2016, it instantly became law in all 28 EU member states. 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 means that on May 25th 2018, the GDPR will be enforced and must be complied with. The spirit of the GDPR focuses on protecting the individual, not applying controls onto companies.

The 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 GDPR, creating a harmonisation of laws across the continent.

Whilst the content of the 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 20 million Euro 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.

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 front and centre in the event of a data breach and has a deep understanding of the organisation's data protection. The DPO's contact details are publicly available for data subjects to access, e.g. on the "Privacy Policy" page of our website, and employees know who the DPO is and how to engage with them.

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 itself.

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: generation, use, storage and disposal. The following sections provide guidance as to the application of this policy through the different life cycle phases of data. 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.

2.1 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 authorized 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 utilized to ensure that only authorized users can access data to which they have been granted explicit access rights.

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 utilized to ensure that only authorized 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 – non-ESF

Record Type	Contract	Regulatory/Funding Body	Retention Period
Personnel Records	N/A	ICO	31 December 2022
Finance Records	N/A	Inland Revenue	31 December 2022
Contract Records	Business Exchange	LLUK	31 December 2022
Contract Records	Youth Contract	EFA	31 December 2021
Contract Records	DWP Employment Experience	DWP	31 May 2020
Contract Records	Business Start-up Support	BC KLWN	31 December 2020

ICO = Information Commissioners Office
EFA = Education Funding Agency
LLUK = Lifelong Learning UK
BC KLWN = Borough Council of Kings Lynn and West Norfolk
DWP = Department of Work & Pensions

Retention Schedule - ESF

Record Type	Contract	Regulatory/Funding Body	Retention Period
Contract Records	Train to Gain	LSC/SFA/ESF	31 December 2022
Contract Records	Leadership & Management	SFA/ESF	31 December 2022
Contract Records	Response to Redundancy (as part of 'Beyond 2010')	EEDA/ESF	31 December 2023
Contract Records	Skills Support for Redundancy	SFA/ESF	31 December 2030
Contract Records	Response to Redundancy 2011	EEDA/ESF	31 December 2023
Contract Records	Response to Redundancy	SFA/ESF	31 December 2022
Contract Records	Skills for Jobs	SFA/ESF	31 December 2022
Contract Records	Integrated Brokerage	EEDA/ESF	31 December 2023
Contract Records	Community Grants	SFA/ESF	31 December 2022
Contract Records	Skills Support for Unemployed	SFA/ESF	31 December 2022
Contract Records	Skills Support for Redundancy	SFA/ESF	31 December 2022
Contract Records	Northamptonshire NEETS	SFA/ESF	31 December 2030
Contract Records	Skills Support for Redundancy	ESFA/ESF	31 December 2030
Contract Records	Skills for the Workforce	SFA/ESF	31 December 2030
Contract Records	Business Start-up Support	BC KLWN	31 December 2020
Contract Records	Building Better Opportunities - SEMLEP	National Lottery/ESF	31 December 2030
Contract Records	Building Better Opportunities – NALEP	National Lottery/ESF	31 December 2030
Contract Records	Building Better Opportunities - GCGP	National Lottery/ESF	31 December 2030

LSC = Learning & Skills Council
SFA = Skills Funding Agency
ESF = European Social Fund
ESFA = Education and Skills Funding Agency
EEDA = East of England Development Agency

The Data Retention Dates are checked and amended when required, during the annual policy review.

The ESF Data Retention Dates are anticipated as of 2018. Prior to any document destruction, the dates are checked on the European Commission website as dates may change.

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 HR will call Shred On Site 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.

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 called Darik's Boot and Nuke. Darik's Boot and Nuke ("DBAN") is a self-contained programme that securely wipes parts of or whole hard disks and other storage media devices. DBAN automatically and completely deletes the contents of any hard disk or storage device that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. DBAN is a means of ensuring due diligence in computer recycling, a way of preventing identity theft and an ideal tool to ensuring sensitive data cannot be restored.

The physical destruction of data media such as physically destroying a Hard Drive or CD ROM is carried out by our IT Department by 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.

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.

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.

The owner of all customer data is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer.

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?
- Is it in line with our business goals and objectives?
- Do customers require or demand access to specific data content.
- What is common local practice? (e.g., pornography is legal in some communities but strongly frowned upon in others.)
- 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. All data found in the processing environment must fall into one of the following categories:

- **Public Company Data/Unclassified** – Public company data is defined as data that any entity either internal or external to TCHC Group can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on TCHC Group nor carry any significant liability. (Examples of Public company data include readily available news, course information, or events.)
- **Proprietary Company Data** – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that TCHC Group is under legal or contractual obligation to protect. The value of proprietary company information to TCHC Group would be destroyed or diminished if such information were disclosed to others. Most TCHC Group sensitive information should fall into this category. Proprietary company information may be copied and distributed within TCHC Group but only to the extent that it is necessary and only to authorised users. Proprietary company information disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary company data include company policies, sales plans, and application source code.)
- **Confidential Company Data** – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on TCHC Group and possibly carry significant civil, fiscal, or

criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Company confidential information must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or encryption keys.)

- **Confidential Customer Data** – Confidential customer data is defined as data that only authorized internal TCHC Group entities or specific authorized external entities can access. The disclosure, use, or destruction of confidential customer data can have adverse affects on TCHC Group and their relationship with their customers, and possibly carry significant liability for both. Confidential customer data is entrusted to and may transit or is stored by TCHC Group (and others) over which they have custodial responsibility but do not have ownership. (Examples of Confidential customer data including customer bank or employee account information, encryption keys, or other data considered private.)
- **Public Customer Data** – Public customer data is defined as data that any entity either internal or external to TCHC Group can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on TCHC Group or the customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by TCHC Group (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

3.4 Data Encryption

3.4.1 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
- 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

3.4.2 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

3.4.3 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.

3.4.4 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 so that only the intended recipient has the ability to decrypt the data.

3.4.5 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.

3.4.6 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 Board of Directors to the Information Commissioner's Office (ICO) in accordance with the GDPR.

3.5 Data Back Up

TCHC data stored locally on in-house servers and remotely on cloud servers are backed up each 24 hour period to secure and encrypted servers. All data back ups are logged and date stamped in order to enable data restore if required through any accidental erasure of data.

3.6 Access Control

3.6.1 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 Chief Executive Officer who may delegate day-to-day technical issues regarding access control.
- All of the Organisation's employees are responsible for controlling access to any information in accordance with this Policy at all times.

3.6.2 Network Access

- Access to the Organisation's network and cloud is controlled by means of individual user log-ins 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 Password Policy. Thereafter, the operating system will automatically prompt for a password change at maximum intervals of 60 days or as determined by the IT Manager.

- 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.
- Log-ins 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 log-ins 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 log-ins and all changes made.
- Anyone who suspects there may have been a breach of network access rules must report it immediately to IT

3.6.3 Access to on-line information

- Information stored on the servers and in the cloud can be 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 Password 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.

3.6.4 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.
- All waste paper containing sensitive business information is to be shredded.

3.6.5 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.
- Avoid leaving your laptop/PC unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the machine
- 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 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 to be carried out by a reputable specialist disposal firm and disposal records are kept for both Information Security and Environmental reasons.
- 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.

- 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 and training manuals
  - The responsibility for arranging these measures lies with the Managing Director

3.6.6 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

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 pornographic or other offensive material via its communications systems.

3.7.1 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 Managing Director 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.

3.7.2 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 Managing Director 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 Managing Director
- 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 Managing Director.

3.7.3 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 really 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 must 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

3.7.4 Password Precautions

All relevant employees of the organisation have been made aware of the following rules, requirements and guidelines with regard to all Passwords and PIN numbers for accessing doors etc:

- Always follow the rules for strong Passwords every time one is created or changed.
- Protect Passwords by making sure nobody is looking over your shoulder when you enter them.
- Keep your Passwords strictly to yourself and avoid revealing them to anyone at all, including colleagues or supervisors.
- Be aware of 'social engineering', when a potential intruder will attempt to get you to reveal a Password by pretending, for instance, to need urgent help getting onto the system. If you are in possession of a Password allowing access to a customer's system, you must exercise extreme caution on this point.
- Do not say your Password out loud, or hint at how you constructed it.
- Do not e-mail or write down or otherwise communicate your Password to anyone.
- Do not keep a note of your Password online or anywhere around your workplace.
- Change a Password if you have reason to believe that someone else knows it. See the Managing Director for this if necessary. If you believe that your Password has become compromised or become aware of the breach of the requirements of this Policy immediately contact the Managing Director for further instructions. Do not try to cover up the incident or ignore it. Information security is a vital factor in the continued success and survival of the organisation and by ignoring a breach of these requirements it could put jobs at risk.
- On leaving the organisation you will be required to reveal all Passwords protecting any files or Directories on any drive owned by the Organisation. Your acceptance of these policies confirms your explicit agreement to do this.

4 Data Sharing Agreement

A Data Sharing Agreement must be in place with each sub-contractor, partner and supplier we work with who processes personal data as part of their contract with TCHC.

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 got some data on 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 3rd 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.

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

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:

- The "right of freedom and expression"
- The need to adhere to legal compliance, e.g. a bank keeping data for 7 years.
- Reasons of public interest in the area of public health
- Scientific, historical research or public interest archiving purposes
- For supporting legal claims, e.g. PPI offerings.

Out of Scope

- Non-electronic documents which are not (to be) filed, (i.e. it's data you can't 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 breeches in our systems so we can quickly and effectively correct.

7 Data Privacy Impact Assessment (DPIA)

A Data Privacy Impact Assessment (DPIA) 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.

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 ro 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.

Once you leave employment from the TCHC Group, you will be asked for consent for us to retain your information for a further 12 months in order that we may contact you should we feel you may be interested in further employment opportunities with us or for any training and development you may want to be referred to. If you do not grant this consent at the end of your employment, then we will only keep your records for one month from your leaving data. We keep information for this period should you request a reference from us or if the inland revenue 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.