Data protection and IT security Policy

This document describes the Cambridge Technical Communicators (CTC) Data protection and IT security policy.

This policy applies to all contractors, employees and casual workers working for our company.

1. Definition of key terms

- **Client** – refers to a customer of CTC who is using our services. Our clients may have their own Data protection and IT security policies, to which all CTC employees and contractors must comply.
- **Client site** – the business premises from where our customer conducts business. You may be required to spend part or all of your contracted working hours at the client site. Refer to your contract document for details.
- **Contractor** – refers to a person CTC has hired on a fixed term contractor or ad-hoc basis to perform a service for our company. This contractor is not an employee of CTC and is responsible for their own income tax payments and Data protection and IT security arrangements. By signing this Data protection and IT security policy, contractors agree to abide by its terms and conditions.
- **Employee** – refers to a person engaged to work for CTC on a permanent, fixed term contract, full-time or part-time basis, where we pay your national insurance and income tax, and any pension contributions. You will also be entitled to vacation time and other benefits. Refer to your contract of employment for details. You must sign and agree to abide by the terms of this Data protection and IT security policy.
- **Casual workers** – hired on an ad-hoc, basis for a number of hours per day, are classed as temporary workers and are not considered as employees of CTC and are not entitled to the benefits available to employees. You must sign and agree to abide by the terms of this Data protection and IT security policy.
- **Remote working** – refers to working from your home or on a client site. We may also refer to this as tele-working. While working remotely, all CTC employees and contractors must take steps to ensure that they are working in a safe and healthy manner.
- **Use of Equipment –** CTC or the client may provide equipment for your use, such as laptops, desktops, computers, mouse and keyboards, telephones or mobile phones. Equipment may also include software applications available for your use. You may also be using your own equipment. Client's may have additional equipment on their site, which you may be expected to wear, use, inspect or come into proximity with. You must abide by any client or CTC policies and guidelines related to the safe use of such equipment. Refer to *Section 4, Use of IT Equipment* for details.
- **Training –** CTC and the client will provide you with training on the use of any equipment. For the use of standard equipment, such as computers and phones, we may expect you to be able to work with this equipment in a safe manner within the minimum level of training or supervision.

2. General principles

I. Most of your work conducted while being employed or contracted by CTC will be at the client's premises or working remote/ from home. This policy covers remote working, commuting to client premises or from home. Where you have been contracted to work from CTC premises or are onsite at CTC premises for meetings, refer to *section 3, Working at CTC Premises* below.

II. Employees and contractors working at home or on a client site are responsible for ensuring that they identify potential risks to their Data protection and IT security and take measures that are reasonable and practical to ensure that they and their colleagues are working in a safe and secure manner.

III. You should at all times act in a responsible and safe manner, so as not to put yourself or your colleagues at risk or cause damage to property or loss of sensitive client information.

IV. Where you become aware of any issues or security risks that may compromise client data, you must notify your CTC Data protection and IT security officer at the earliest available opportunity.

V. If you are working at a client site, you must read the client's Data protection and IT security guidelines, procedures and policies.

VI. Contractors should ensure that adequate insurance is in place to cover them for incidents related to their Data protection and IT security when working from home or at another site, while commuting to work or while working at a client site.

VII. All CTC employees and contractors will at all times act in a safe and responsible manner as a CTC representative in the course of their contracted employment.

3. Working at CTC premises

I. Where you have been contracted to work from CTC premises or are onsite at CTC premises for meetings, you must abide by any instructions provided to you while onsite, in addition to those outlined in this policy.

II. While onsite you will act at all times in a responsible manner and avoid actions that may put yourself or others at risk or result in loss of confidential client information.

III. You will notify your nominated Data protection and IT security officer promptly of any defects or omissions at the site that you are aware of which might result in risks to security or and safety.

4. Use of IT Equipment

I. CTC or the client may provide equipment for your use, such as laptops, desktops, computers, monitors, mouse and keyboards, projectors, printers, telephones or mobile phones.

II. Equipment may also include software applications available for your use.

I. IT equipment must be used in a responsible manner and not subjected to undue stress, for example, by exposing to extremes in temperature or humidity, or placing equipment in direct sunlight or in contact with heating equipment or water.

II. Do not remove any labelling applied to equipment for identification purposes.

III. Do not connect your CTC or client equipment to any unauthorised devices, including printers and storage devices.

IV. Complete any mandatory health and safety assessments or training courses to ensure your equipment is safe for use and that you are using it properly.

V. You will follow the client's instructions related to the safe use of any IT equipment provided to you. In all instances the client is responsible for ensuring that you have been adequately trained in the use of such equipment, and for supervising your usage. If you suspect any deficiencies or omissions on the part of the client in your training and supervision to use such equipment, you will notify the client and your CTC Data protection and IT security officer promptly.

VI. We expect you to know how to use basic equipment such as computers, laptops, phones or mobile phones in a safe and secure manner. If you are unfamiliar with the usage of such devices, please notify your CTC Data protection and IT security Officer, so that appropriate training can be arranged.

VII. You will notify CTC or the client promptly of any defects to equipment:

a. Where you are using equipment provided to you by CTC, CTC is responsible for ensuring that such equipment is free from defects and safe to use;

b. Where you are using equipment provided to you by the client, the client is responsible for ensuring that such equipment is free from defects and safe to use;

c. Where you are using your own equipment in the course of your contracted employment with CTC, you are responsible for ensuring that such equipment is free from defects and safe to use.

VIII. Take reasonable precautions to prevent theft or loss of CTC or Client equipment:

a. Ensure that portable devices such as laptops are appropriately locked away or secured (e.g. using a security cable).

b. Make sure that only authorised staff or persons known to you have access to rooms where IT equipment is kept

5. Use of IT equipment when working remotely

I. If you need to work from a remote location (e.g. from home) you must first obtain permission from your line manager or above to be set up to do so.

II. Be aware of the additional risks associated with remote working. For example, how secure are your premises, or the location in which any IT equipment is currently being stored?

III. In particular, check that:

a. You can secure premises/rooms where IT equipment is kept, to prevent unauthorised access:

b. If you are using your personal computer (not owned by CTC or the client) to log in to the client's network remotely, ensure that your PC has up-to-date anti-virus software and does not store any sensitive client data.

IV. You will need to be especially vigilant when IT equipment (such as laptops, handheld devices or removable disks) is in transit. For example, when equipment or sensitive information is kept in motor

vehicles, carried while using public transport, used at conference centres and meeting places, or stored at hotels, make sure that you take additional precautions:

a. Never leave equipment unattended, for example on the back seat of your car or on a chair or table in any public location.

b. Make sure that any sensitive information (e.g., personal or confidential data) on laptops and portable storage devices is encrypted and/or password-protected.

c. Do not leave equipment locked overnight in a motor vehicle. Always take equipment with you to a secure location.

d. When visiting clients or high-crime neighbourhoods, use discretion and do not openly display laptops or other IT equipment.

V. Loss or theft of any CTC or client computing device must be reported immediately to CTC or the client.

6. Access to sensitive information

I. Due to the nature of work in our industry, those engaged in technical communications and related fields, such as graphic design, marketing, web development, translation, may have access to sensitive client information. Examples are included below:

a. Customer names, contact or account details – often available in screens and databases linked to applications you may be documenting

b. Client internal, confidential documents – including specifications, plans, drawings, diagrams, proposals and internal documents, not intended for external usage

c. Patented and other sensitive information – which may cause considerable damage to the organisation and financial loss if these were to fall into the wrong hands.

d. Access to usernames, passwords and other details for accessing secure systems.

II. Any such sensitive information should not be displayed under any circumstances in external, customer-facing documentation.

III. You will take steps to ensure that any sensitive information provided to you is stored securely and disposed of after use.

IV. Sensitive information must not be stored on an personal equipment or computers under any circumstances. If a member of a Client organisation or CTC request or send you sensitive data to your personal account, you must notify your CTC data protection officer promptly.

V. You will not pass on any sensitive information to any third parties without the written agreement of CTC or the client.

VI. You will ensure that any documents that contain sensitive or confidential information are appropriately marked as [CONFIDENTIAL] or [INTERNAL USE ONLY]

VII. If any communication with other parties in which sensitive or confidential information is shared, you will ensure that headings of emails/letters or any other such communications will be appropriately marked as [CONFIDENTIAL] or [INTERNAL USE ONLY]

VIII. You will ensure that such information is only shared over secure channels, for example through a Virtual Private Network (VPN) connection, secure portal or other means provided by CTC or the client. Under no circumstances should you share sensitive information over a non-secure connection, such as using your personal email account.

7. Keeping information secure

I. When you are away from your desk, ensure that your computer is locked (on your keyboard, hold down the *Ctrl* key and press *Alt* and *Delete*) so that no-one can gain access to your files.

II. Do not leave confidential or sensitive information on display on your desktop or on screen where passers-by may be able to view it.

III. When you will be away from your desk for more than 15 minutes, turn off your monitor to save energy

IV. Do not allow your CTC or client equipment to be used by anyone other than CTC or client employees, contractors or volunteers, all of whom must have been assigned their own login ID.

8. Use of passwords

I. Where passwords are required to access secure client or CTC services, please ensure that you adhere to the rules in this section.

II. Chose a password that is unique - do not use the same password for both CTC/Client and personal use, or the same password in rotation.

III. Keep your password personal and secret – never write it down or share with anyone.

IV. Chose a password that is hard to guess (e.g. don't use common words, names, personal information, initials or dates).

V. If at any time you suspect someone else knows your password, then change it immediately.

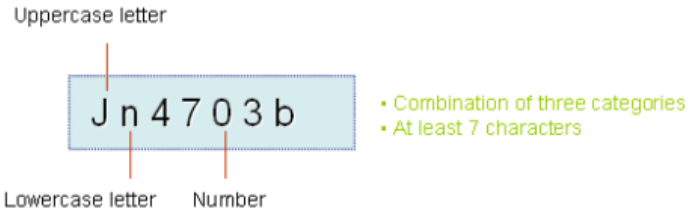
VI. Passwords that are used to access secure IT facilities should:

a. contain at least **seven** characters (combination of alpha and numeric characters).

b. contain a combination of characters from any **three** of the following categories:

- uppercase letters (e.g., A, B, C...Z)
- lowercase letters (e.g., a, b, c…z)
- numbers (e.g., 0, 1, 2…9)
- non-alphanumeric characters (e.g., #, &, $, %)

These rules are designed to ensure that your passwords are sufficiently complex and hard to guess. Below is an example of a valid password:



9. Copying data to a memory stick, computer disk or other portable storage device

I. If you are copying sensitive data to CD or a portable device (e.g., USB stick or flash drive) ensure that the device is password-secured.

II. You may be requested to only use portable storage devices provided by CTC or the Client. These devices are encrypted and password protected.

III. Any data that could be considered sensitive (e.g., personal or confidential data) should not be transferred or stored using these devices, unless you have prior approval. Once you have finished using the portable device, any information left on it should be deleted

IV. Removable media is not robust and great care must be taken when transporting live or working data or files. If the media becomes corrupted or damaged then valuable information which has taken a long time to prepare could be lost.

10. Making backup copies of information on your computer

I. If you are working locally on your computer, make sure that a copy of your latest files is always backed up at the end of the day to the CTC or Client network or site provided to you for this purpose.

II. You will take steps to ensure that your Client line manager or CTC contact are provided with details of where the latest files you are working on are located, and that they have been provided with any passwords required to open these files, if protected.

I acknowledge the following:

I have read CTC's Data protection and IT security Policy	
I have read the client's Data protection and IT security Policy (where applicable)	
I have taken steps to ensure that I am working in a safe and secure manner	
I have received training on the use of any specialised equipment related to the performance of my duties (where applicable)	
I will raise any issues related to my Data protection and IT security promptly with the nominated CTC Data protection and IT security officer, as soon as these issues come to my attention	
I will take steps to ensure that I continue to work in a safe and secure manner. I will identify risks related to the Data protection and IT security of myself and my colleagues and notify CTC in writing of any potential risks	

Signed _____

Date: _____

Overall and final responsibility for Data protection and IT security is that of:	Warren Singer, Director, CTC
Day-to-day responsibility for ensuring this policy is put into practice is delegated to:	All CTC employees, contractors and casual workers

Data protection and IT security Objectives	**Document reference**	**Delivery details**
To prevent loss or theft of client or CTC equipments	CTC Data protection and IT security Policy	Relevant risk assessments completed and actions arising out of those assessments implemented. (Risk assessments are reviewed every year, or earlier if working habits or conditions change.)
To prevent loss or theft of secure/sensitive client or CTC data.	CTC Data protection and IT security Policy	Staff and contractors given necessary Data protection and IT security induction and provided with appropriate training and equipment. We will ensure that suitable arrangements are in place to cover employees engaged in remote work or on a client site.
To engage and consult with employees on day-to-day Data protection and IT security conditions and provide advice and supervision.	CTC Data protection and IT security Policy	Staff routinely consulted on Data protection and IT security matters as they arise but also formally consulted at regular Data protection and IT security performance review meetings or sooner if required.

Signed:	*Warren Singer*	Date:	31/03/19	
Subject to review, monitoring and revision by:	Warren Singer	Every:	12	months or sooner if work activity changes