Cambridge & Ely
Child Contact Centre

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

Information Security Policy

Introduction

This information security policy is a key component of Cambridge & Ely Child Contact Centres management framework. It sets the requirements and responsibilities for maintaining the security of information within Cambridge & Ely Child Contact Centres. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

Purpose

This policy is intended to support Cambridge & Ely Child Contact Centres business objectives and, without undue restrictions, protect its staff, clients, contractors, third parties and the business from illegal or damaging events or actions by individuals, either knowingly or unknowingly.

The objective of this policy is to define the Cambridge & Ely Child Contact Centres' procedures to protect the confidentiality, integrity, and availability of Cambridge & Ely Child Contact Centres' information assets, its reputation, and the safety of all its stakeholders. Everyone who works in or with the Company has a duty and a responsibility to comply with these policies.

Applicability

The policy applies to the use of all Cambridge & Ely Child Contact Centres IT equipment and information systems belonging to or managed by the company, including but not limited to laptops, mobile devices (such as smart-phones), removable media, third-party systems and any cloud-based infrastructure, platforms, or services.

This policy is applicable to all Cambridge & Ely Child Contact Centres staff both permanent, temporary and volunteers who provide services. It is the responsibility of all such individuals to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty, employees should consult the centre coordinator.

Aim and Scope of this policy

The aims of this policy are to set out the rules governing the secure management of our information by:

- preserving the confidentiality, integrity and availability of our business information.
- ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- ensuring an approach to security in which all members of staff fully understand their own responsibilities.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

- creating and maintaining within the organisation a level of awareness of the need for information.
- detailing how to protect the information assets under our control.

This policy applies to all information/data, information systems, networks, applications, locations and staff of Cambridge & Ely Child Contact Centres or supplied under contract to it.

Responsibilities

Ultimate responsibility for information security rests with the Trustees but the centre coordinator shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this Policy and for recommending appropriate risk management measures is held by the Centre coordinator. The Policy shall be reviewed by the Committee at least annually.

Coordinators are responsible for ensuring that their staff, and contracts are aware of: -

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to access advice on information security matters.

All staff shall comply with the information security policy and must understand their responsibilities to protect the Centre's data. Failure to do so may result in disciplinary action.

Coordinators shall be individually responsible for the security of information within their business area.

Each member of staff shall be responsible for the operational security of the information systems they use.

Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity, and availability of the information they use is maintained to the highest standard.

Access to the organisation's information systems by external parties shall only be allowed where a contract that requires compliance with this information security policy is in place. Such a contracts shall require that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

To ensure compliance, the following is needed:

- Appoint a member with specific responsibilities for security – the risk owner.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

- Appoint a person responsible for day–to-day security.
- Identify individuals responsible for specific information assets such as: family information, staff, or finance information. They need to be able to understand the threats likely to compromise the information.
- Ensure that all individuals with designated security responsibilities undertake appropriate training for their role.

Risk Assessment and Management

Cambridge & Ely Child Contact Centres will adopt a risk assessment methodology as part of a holistic risk management approach covering all areas of protective security across its organisation. It will include a risk register (with assigned risk owners) recording any specific vulnerabilities or security risks, the control measures taken to mitigate these risks, and any adjustments over time following changes to the threat environment. Subject to security considerations, the risk register should be made widely available within the organisation to ensure all business units have an input It will include:

- A statement of the IT assets deployed by Cambridge & Ely Child Contact Centres – the asset register.
- A statement of the threats faced by Cambridge & Ely Child Contact Centres.
- A statement of the impacts of compromise of the information assets.
- A statement of the tolerable level of risk (the risk appetite.)
- Record the application of proportionate selection of technical, procedural, personnel and physical security controls to manage the identified risks to a level that the business can tolerate.

For all projects that include the use of personal information Cambridge & Ely Child Contact Centres must assess the privacy risks to individuals in the collection, use and disclosure of the information and a Privacy Impact Assessment (PIA) / Data Protection Impact Statement (DPIA), as recommended by the Information Commissioner, must be carried out as a minimum.

Can regularly audit information assets and ICT systems to check compliance and extract data in the event of an incident.

Where shared systems or services are used, Cambridge & Ely Child Contact Centres must satisfy themselves that the use of these systems or services can be managed within its own risk appetite.

Legislation

Cambridge & Ely Child Contact Centres is established as a Charity

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

Cambridge & Ely Child Contact Centres is required to abide by certain UK and international legislation.

In particular, Cambridge & Ely Child Contact Centres is required to comply with:

- The Data Protection Act (2018).
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.
- The Copyright, Designs and Patents Act (1988).
- The Computer Misuse Act (1990).
- The Health and Safety at Work Act (1974).
- Human Rights Act (1998).
- Freedom of Information Act 2000.

Personnel Security

Contracts of Employment, paid or unpaid

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a security and confidentiality clause.
- References for new staff shall be verified and a passport, driving license or other document shall be provided to confirm identity.
- Information security expectations of staff shall be included within appropriate job definitions.
- Whenever a staff member leaves the company, their accounts will be disabled the same day they leave.

Information Security Awareness and Training

- The aim of the training and awareness programmes are to ensure that the risks presented to information by staff errors and by bad practice are reduced.
- Information security awareness training shall be included in the staff induction process and shall be carried out annually for all staff
- An on-going awareness programme shall be established and maintained to ensure that staff awareness of information security is maintained and updated as necessary.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Coordinator, Individual and Cambridge & Ely Child Contact Centres intellectual property rights shall be always protected.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

- Users breaching this requirement may be subject to disciplinary action.

Access management

Physical Access

- Only authorised people who have a valid and approved business need shall be given access to areas containing information systems or stored data.

Identity and passwords

- Passwords must offer an adequate level of security to protect systems and data.
- All passwords shall be eight characters or longer and contain at least two of the following: upper case letters, lower-case letters, and numbers
- All administrator-level passwords shall follow NCSC guidelines: https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach

User Access

- Access to information shall be based on the principle of "least privilege" and restricted to authorised users who have a need to access the information.

Administrator-level access

- Administrator-level access shall only be provided to individuals with a business need who have been authorised by Cambridge & Ely Child Contact Centres Coordinator.
- A list of individuals with administrator-level access shall be held by Cambridge & Ely Child Contact Centres Coordinator and shall be reviewed every 6 months
- Administrator-level accounts shall not be used for day-to-day activity. Such accounts shall only be used for specific tasks requiring administrator privileges.

Application Access

- Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g., systems or database administrators.
- Authorisation to use an application shall depend on a current licence from the supplier.

Hardware Access

- Where indicated by a risk assessment, access to the network shall be restricted to authorised devices only.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

System Perimeter access (firewalls)

- The boundary between business systems and the Internet shall be protected by firewalls, which shall be configured to meet the threat and continuously monitored.
- All servers, computers, laptops, mobile phones, and tablets shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.
- The default password on all firewalls shall be changed to a new password that complies to the password requirements in this policy, and shall be changed regularly
- All firewalls shall be configured to block all incoming connections.
- If a port is required to be opened for a valid business reason, the change shall be authorised following the system change control process. The port shall be closed when there is no longer a business reason for it to remain open.

Monitoring System Access and Use

- An audit trail of system access and data use by staff shall be maintained wherever practical and reviewed on a regular basis.
- Cambridge & Ely Child Contact Centres reserves the right to monitor and systems or communications activity where it suspects that there has been a breach of policy in accordance with the Regulation of Investigatory Powers Act (2000).

Asset Management

Asset Ownership

- Each information asset, (hardware, software, application, or data) shall have a named custodian who shall be responsible for the information security of that asset.

Asset Records and Management

- An accurate record of Cambridge & Ely Child Contact Centres information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.

Asset Handling

- Cambridge & Ely Child Contact Centres shall identify particularly valuable or sensitive information assets using data classification.
- All staff are responsible for handling information assets in accordance with this security policy. Where possible the data classification shall be marked upon the asset itself.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

- All company information shall be categorised according to the risk assessment and shall be handled according to the risk appetite defined in that policy.

Removable media

- Only Cambridge & Ely Child Contact Centres approved removable media (such as USB memory sticks) shall be used to store Centre data it will be encrypted, and its use shall be recorded.
- Removable media of all types that contain software or data from external sources, or that has been used on external equipment, require the approval of the Coordinator before they may be used on business systems. Such media must be scanned by anti-virus before being used.
- Where indicated by the risk assessment, systems shall be prevented from using removable media.
- Users breaching these requirements may be subject to disciplinary action.

Local Data Storage

- Data is stored on the Cloud

Data Protection

- Data in transit will always be protected by encryption (TLS or IPsec)
- Data at rest will be protected as follows:
    - Personal data will be password protected.
    - Other sensitive information, i.e., information where the confidentiality impact is assessed at medium or above, will be password protected.0
    - All other data will be protected by restricting access to identified and authenticated authorised individuals.

External Cloud Services

- Where data storage, applications or other services are provided by another business (e.g., a 'cloud provider') there must be independently audited, written confirmation that the provider uses data confidentiality, integrity and availability procedures which are the same as, or more comprehensive than those set out in this policy.

Protection from Malicious Software

- The business shall use software countermeasures, including anti-malware, and management procedures to protect itself against the threat of malicious software.
- All computers, servers, laptops, mobile phones, and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

- All anti-malware software shall be set to:
    - scan files on-access
    - automatically check for, daily, virus definitions and updates to the software itself and install new versions when they become available
    - block access to malicious websites

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Centre Coordinator.
- All other information security incidents shall follow an SIR (Security Incident Response) procedure which require:
    - If required because of an incident, data will be isolated to facilitate forensic examination.
    - Information security incidents shall be recorded in the Security Incident Log.
    - The risk assessment and this policy shall be updated if required to reduce the risk of a similar incident re-occurring.
- Identify and assign information security roles and responsibilities appropriate to the size, structure, and business function of their organisation.
- Adopt policies, procedures, and controls to ensure information assets are identified, valued, handled, stored, processed, transmitted, shared, and destroyed in accordance with legal requirements.
- Manage the risks associated with digital continuity and records management in respect of all data held electronically, particularly in the event of upgrades in technology, transferral of data into archives and the overall life cycle of data.
- Assess any security and business risks before deciding to outsource or offshore information and/or services. Data or services that relate to or directly support national security should not normally be off shored.

Privacy Statements

The Contact Centre must provide a privacy statement to all data subjects, for which we hold data. This should be in line with ICO guidance about following GDPR.

Procedures must be in place covering the receipt, storage, correction, and deletion of personal, including special category, data.

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

Valuing and Classification Assets

The Contact Centre must ensure that information assets are valued, handled, shared, and protected in line with the standards and procedures set out in legal obligations and undertakings,

To comply with this requirement, Cambridge & Ely Child Contact Centres will ensure that:

- Information and other assets are valued according to the definitions the classification policy and are clearly and conspicuously marked. Where this is impractical (e.g., a building or physical asset) staff must be made aware of the protective controls required.
- Assets are protected in line with the risk appetite and countermeasures, defined in the risk assessment, throughout their life cycle from creation to destruction to ensure a proportionate level of protection against the real and/or anticipated threats faced by such assets.
- Access to sensitive assets is only granted based on a genuine need to know and an appropriate level of personnel security control.
- Where information is shared for business purposes Cambridge & Ely Child Contact Centres must ensure the receiving party understands the obligations and protects the assets appropriately.

Risk Assessment and Accreditation of ICT Systems

Business Continuity and Disaster Recovery Plans

- The organisation shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems, and networks.

The following arrangement shall be followed:

Risk	Likelihood Score	Mitigation Plan
Loss of staff: As an organisation many skill sets are very critical to the organisation.	B. High Impact, Low Likelihood.	Capture as much information as possible. Prioritise having staff that provide redundancy.
Loss of premises: e.g., building burns down.	B. High Impact. Low Likelihood.	Information is stored on electronic devices with a backup held offsite. There may be an operational delay, but information would not be lost.
Loss of key supplier:	D. Low Impact. Low Likelihood.	Contractual arrangement shall be put into place which supports the

Phone: +44 7812 157448
Email: mary@ceccc.org.uk

Registered Charity Number: 1145344
Company Registration Number: 7464402

		transfer of services to alternative suppliers if required.

Implementation

Reviewed by		
Name Bridget Giltinane	Signature: B.Giltinane	Date: 18.08.25
This Policy will be reviewed no less than once every three years.		