**West Wilts Child Contact Centre**

**Information Security Policy**

**1. Introduction**

This information security policy is a key component of the West Wilts Child Contact Centre’s (WWCCC) management framework. It sets the requirements and responsibilities for maintaining the security of information within WWCCC. This policy may be supported by other policies and by guidance documents to assist putting the policy into practice day-to-day.

**2. Purpose**

The objective of this policy is to define the WWCCC’s policies in order to protect the confidentiality, integrity and availability of WWCCC’s information assets, its reputation and the safety of all its clients and stakeholders. Everyone who works in or with the Centre has a duty and a responsibility to comply with these policies.

**3. Application**

This policy applies to all information systems owned and used by WWCCC. It includes computers, telephones and paper records and any other data storage systems and methods. All volunteers will be made aware of this policy and its implications.

The policy restricts the use of private telephones and computers to information that is not sensitive.

All suppliers of equipment to WWCCC who made need access to computer systems will be made aware of this policy and that any information that they may see in the course of their work must net be recorded or divulged to any other person.

**4. Aim and scope of this policy**

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

* preserving the **confidentiality, integrity and availability** of our contact centre information
* ensuring that all volunteers 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 volunteers fully understand their own **responsibilities**
* 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 and to volunteers of the WWCCC. It also applies to contractors who may be involved in the supply. Installation or support or repair of systems.

**5. Responsibilities**

Ultimate responsibility for information security lies with the management committee.

Each volunteer is responsible for the security of information on centre system that they are authorised to access. This includes centre computer(s) telephones and paper records.

The password to the centre’s computer which holds centre user’s records is only known to the coordinator. A sealed copy of the password is kept by one other management committee member. This is strictly for emergency use should the coordinator be unavailable for an extended period. The sealing is achieved by the coordinator signing the envelope partly over the main body of the rear of the envelope and partly over the flap. Then putting Selotape across his/her signature. It will then be apparent if the envelope has been opened.

If there is a need to open the envelope for any reason the event shall be reported to the next meeting of the management committee and the reason and date of opening recorded in the minutes of the meeting.

During contact sessions the team leader is responsible for security. Only the attendance sheet shall be on the reception desk and kept ‘face down’ expect when recording an arrival or departure. Once centre users have entered the premises the computer shall be kept out of sight as much as possible and the data only consulted if necessaryu shall be securely out of sight as much as possible and only consulted if necessary.

Users of centre mobile phones shall all reasonable steps to avoid their loss. Contact lists must not be stored on the centre’s phones. Any new phones purchased for use of the centre must be ‘pin’ protected.

 **6. Risk Assessment and Management**

The WWCCC 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 the CCC – the asset register.
* A statement of the threats faced by the CCC
* A statement of the impacts of compromise of the information assets
* A statement of the tolerable level of risk (the risk appetite)

**6. Legislation**

The West Wilts Child Contact Centre is a registered charity.

WWCCC is required to abide by certain UK, European Union and international legislation.

In particular, WWCCC is required to comply with:

* + The Data Protection Act (2018) (Including GDPR)
	+ 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)

**Personnel Security**

Volunteer Agreement

* Volunteer security requirements shall be addressed at the recruitment stage.
* References for new volunteers shall be verified and a passport, driving license or other document shall be provided to confirm identity.
* Information security expectations of volunteers shall be included within appropriate job definitions.

**Information Security Awareness and Training**

All new volunteers of the centre’s information security policies and requirements. All volunteers will be trained in this policy on its introduction and again on any revision.

**Intellectual Property Rights**

* The organisation shall ensure that all software is properly licensed and approved by the Coordinator / administrator. Individual and WWCCC intellectual property rights shall be protected at all times.
* Users breaching this requirement may be subject to disciplinary action.

**Access management**

Only the centre co-ordinator knows the password to the centre’s computer. She is authorised to load data, make amendments to keep the data up to date and to delete out of date records. She is authorised to back up date to the icloud or other back up system which must be password protected. Any information on paper records shall be locked away when not in use.

All passwords shall consist of eight or more characters. They shall contain at least two of the following:

Upper case letters

Lower case letters

Numbers

A sealed copy of all the passwords shall be held by another member of the management committee and may only be opened and used for emergency access to data in the absence of the coordinator.

If the coordinator leaves the post the passwords shall be changed. (If necessary) using the emergency access passwords held by another member of the committee.

During contact sessions the session team leader and on duty volunteers shall have access to the information required to run the session smoothly using the centre’s computer. While centre users are on the premises this information shall be kept securely out of the sight of centre users. The only paper record is the attendance sheet on the front desk.

All volunteers will be made aware that all centre user information is confidential and can only be released if required to do so by law or to support a child protection issue.

**Handling Centre Information Assets**

Only the centre coordinator may keep and use the centre’s data computer. Sensitive information on centre users may not be held on private computers.

Only centre owned mobile phones may be used to contact centre users.

Any use of data sticks must be recorded and any information must be encrypted.

**Private Computers**

Emails are not guaranteed totally secure.

Management committee minutes and agendas may be circulated using private computers. Providing they do not contain information be which centre users can be identified. ie use family ‘x’ and not the full surname.

**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 (Information Commissioner’s Office) ICO guidance about following the General Data Protection Regulation (GDPR).

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

The annual report is NOT confidential and may be given to any person having reasonable grounds for wanting to see it. Policies and Procedures may be requested by centre users and others and therefore are not confidential and may be stored on private computers.

**Social Media Accounts**

Social media accounts shall not be used by the centre.

**Physical Threats**

Any device capable of being connected to the internet shall have antivirus protection installed. Updates shall be run as soon as possible.

The centre’s management committee shall consider an uninterrupted power supply for any mains driven computer equipment.

**Networks**

West wilts child contact centre does not run any networks. The security required must be reviewed and this policy updated before any network is installed.

System Change Control

* Changes to information systems, applications or networks shall be reviewed and approved by the WWCCC management committee

Accreditation

* The WWCCC shall ensure that all new and modified information systems, applications and networks include security provisions.

Software Management

* All application software, operating systems and firmware shall be updated on a regular basis to reduce the risk presented by security vulnerabilities.
* All software security updates/patches shall be installed within 7 days of their release.
* Only software which has a valid reason for its use shall be installed on devices used for contact centre purposes purposes
* Users shall not install software or other active code on the devices containing business information without permission from the centre coordinator.
* For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for contact centre purposes purposes.

Data Storage

Data stored on the centre’s computer shall be backed up regularly. This can be externally to an icloud or similar. Only systems with a high reputation may be used.

**Disaster Recovery Plan**

**Possible Incident**

Theft, hard drive crash, accidental or malicious destruction of computer.

**Recovery**

Load data from icloud or similar to a new computer.

**Loss or theft of paper records Including referrals court orders etc claimed to have been posted but not received.**

All sensitive documents shall be scanned and backed to the icloud or similar as soon as possible. Loss of paper documents including the non delivery of items claimed to have been posted. This non delivery shall be discussed with the sender and duplicates requested.

Loss of paper documents shall be considered as possible breach of data. Suspected or definite hacking of the centre’s computer or icloud is a breach of data **and the data breach policy must be implemented.**

**Letters sent via Royal Mail to centre users shall carry the word confidential and request if undelivered to return to our current PO Box.**

Signed……………………………………………Signed…………………………………….

Date……………………………………………….Date………………………………………

Position……………………………………………Position……………………………….

.

.