Birmingham Child Contact Centre

Information Security Policy

To be used in conjunction with BCCC's Privicy Policy.

Introduction.

This information security policy is a key component of the Birmingham Child Contact Centre (BCCC) management framework. It sets the requirements and responsibilities for maintaining the security of information within BCCC. 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 BCCC objectives and, without undue restrictions, protect its volunteers and service users and BCCC from illegal or damaging events or actions by individuals, either knowingly or unknowingly.
The objective of this policy is to protect the confidentiality, integrity and availability of BCCC's information assets, its reputation and the safety of all its volunteers and service users. Everyone who uses or volunteers in BCCC has a duty and a responsibility to comply with these policies.

Applicability

The policy applies to the use of all BCCC IT equipment and information systems belonging to or managed by the centre including but not limited to: laptops, computers, telephones, mobile devices (such as smart-phones), removable media, or services e.g. email, printers/scanners

This policy is applicable to all BCCC volunteers. It is the responsibility of all individuals to read and understand this policy, and to conduct activities in full accordance with it. If there is any uncertainty the Volunteers & Families Coordinator / Duty Coordinator should be contacted.

Aim and Scope of this policy

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

- preserving the **confidentiality, integrity and availability** of our information
- ensuring that all members 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 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 and members of BCCC.

Responsibilities
Ultimate responsibility for information security rests with the Management Committee who shall be responsible for managing and implementing the policy and related procedures.

Responsibility for maintaining this policy, Risk Register and for recommending appropriate risk management measures is held by the Management Committee. Both the Policy and the Risk Register shall be reviewed by the Management Committee at least annually.

The Management Committee is responsible for ensuring that all volunteers are aware of:-

- The information security policy
- Their personal responsibilities for information security
- How to access advice on information security matters

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

The Coordinator shall be individually responsible for the security of information within their area.

Each volunteer 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 are maintained to the highest standard. In addition they should:

- Identify individuals responsible for specific information assets such as: Referrals Coordinator, Volunteers & Families Coordinator, Duty Coordinator(s). Secretary and Treasurer. They need to understand the threats likely to compromise information held.
- Ensure that all individuals with designated security responsibilities undertake appropriate training for their role.

Risk Assessment and Management

BCCC will adopt a risk assessment methodology as part of an holistic risk management approach covering all areas of protective security across its organisation. It will include a risk register 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.

- A statement of the IT assets deployed by BCCC – the asset register.
- A statement of the threats faced by BCCC
- A statement of the impacts of compromise of the information assets
- A statement of the tolerable level of risk
- Record the application of proportionate selection of technical, procedural, personnel and physical security controls to manage the identified risks;

For all projects that include the use of personal information BCCC 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.
Has the ability to 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, BCCC must satisfy themselves that the use of these systems or services can be managed within its own risk appetite.

Legislation

- BCCC is established as a voluntary organisation
- BCCC is required to abide by certain UK, European Union and international legislation.
- In particular, BCCC is required to comply with:
- The Data Protection Act (2018) (Including General Data Protection Regulations)
- 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

Volunteer Agreement

- Volunteer security requirements shall be addressed at the volunteer training stage and all training shall contain a security and confidentiality reminder/focus.
- References for volunteer shall be verified and a passport, driving licence or other appropriate document shall be provided to confirm identity.
- Information security expectations of volunteers shall be included within appropriate volunteer job descriptions.

Information Security Awareness and Training

- The aim of training and awareness programmes are to ensure that risks associated with volunteer errors and by bad practice are reduced.
- Information security awareness training shall be included in the volunteer refresher courses and all staff are required to attend on a minimal annual basis.

Intellectual Property Rights

- The organisation shall ensure that all software is properly licensed and approved by the Mangement Committee. Individual and BCCC intellectual property rights shall be protected at all times.
- 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
- Passwords shall be eight characters or longer and contain at least two of the following: upper case letters, lower-case letters and numbers
- Administrator-level passwords shall follow National Cyber Security Council guidelines (see https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach)
- All individual users shall use uniquely named user accounts

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.

Computer access

- A list of individuals with access shall be held by the Volunteers and Families Coordinator and Secretary of BCCC and shall be reviewed every 12 months

Hardware Access

- Where indicated by a risk assessment, access to a computer will be restricted to authorised persons only.

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 computers, laptops, mobile phones, tablets and other internet enabled devices e.g. printer/scanner multi function devices shall have a firewall enabled, if such a firewall is available and accessible to the device's operating system.

Monitoring System Access and Use

- An audit trail of system access and data use by volunteers shall be maintained wherever practical and reviewed on a regular basis.
- BCCC reserves the right to monitor 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 BCCC information assets, including source, ownership, modification and disposal shall be maintained.
- All data shall be securely wiped from all hardware before disposal.

Asset Handling

- BCCC shall identify particularly valuable or sensitive information assets through the use of data classification.
- All volunteers are responsible for handling information assets in accordance with this security policy.
- All company information shall be categorised according to the risk assessment and shall be handled according to the risks defined in that policy.

Removable media

- Only BCCC approved removable media (e.g. USB memory sticks) shall be used to store BCCC data 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 BCCC's 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.

Mobile working

- Where necessary, staff may use charity-supplied mobile devices such as phones, tablets and laptops to meet their job role requirements
- Use of personal mobile devices for Contact Centre purposes (whether Contact Centre owned or personal devices) requires the approval of BCCC's Management Committee.
- Such devices must have anti-malware software installed (if available for the device), must have PIN, password or other authentication configured. They must also comply with the software management requirements within this policy.
- Users must inform BCCC's Management Committee immediately, if the device is lost or stolen.

Personal devices / Bring Your Own Device (BYOD)

- Where necessary, staff may use personal End User Devices (EUDs), i.e., mobile phones, laptops, tablets etc, to access email. Content may only be stored on devices approved by the Management Committee. The device must be recorded in the asset register and must be configured to comply with the relevant sections of this policy.
- No other personal devices are to be used to access BCCC information.

Social Media

- Social media may only be used for business purposes by using official Contact Centre social media accounts with authorisation. Users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

- Access to all BCCC business facilities and functions will be restricted to duly identified and authenticated authorised individuals.
- Social media accounts used by BCCC shall be protected by strong passwords in-line with the password requirements for administrator accounts.
- Personal Social Media Account users shall behave responsibly while using any social media whether for Contact Centre or personal use, bearing in mind that they directly or indirectly represent BCCC. If in doubt, consult the BCCC Coordinator.
- Users breaching this requirement may be subject to disciplinary action.

Physical and Environmental Management

- In order to minimise loss of, or damage to assets, equipment shall be physically protected from threats and environmental hazards. Physical security measures should be applied if necessary e.g. lockers, safes, etc.

Computer and Network Management
Operations Management

- Management of computers and networks shall be controlled through standard documented procedures that have been authorised by BCCC's Management Committee.

System Change Control

- Changes to information systems and applications shall be reviewed and approved by BCCC's Management Committee.

Accreditation

- BCCC shall ensure that all new and modified information systems and applications 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 at the earliest convenience following their release.
- Only software which has a valid business reason for its use shall be installed on devices used for charity purposes
- Users shall not install software or other active code on the devices containing charity information without permission from the Management Committee.
- For the avoidance of doubt, all unnecessary and unused application software shall be removed from any devices used for Charity purposes.

Local Data Storage

- Data stored on Contac Centre premises shall be backed up regularly.
- A backup copy shall be held in a different physical location to the Contact Centre.
- Backup copies of data shall be protected and comply with the requirements of this security policy and be afforded the same level of protection as live data.

Data Protection

- Data in transit should be protected as far as practicable e.g. case, locked boot,
- Data at rest will be protected as follows:
    - Personal data will be encrypted, (this is in line with GDPR requirements) and keys held by trusted custodians.
    - Other sensitive information, i.e., information where the confidentiality impact is assessed at medium or above, will be encrypted and keys held by trusted custodians.
    - All other data will be protected by restricting access to identified and authenticated authorised individuals.

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, laptops, mobile phones and tablets shall have anti-malware software installed, where such anti-malware is available for the device's operating system
- 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

Vulnerability scanning

- The results of the scan and any changes made shall be reflected in the company risk assessment and security policy as appropriate.

Information security incidents

- All breaches of this policy and all other information security incidents shall be reported to the Centre Chairman and Management Committee.
- All other information security incidents shall follow a SIR (Security Incident Response) procedure which requires:
    - In the event 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.
    - BCCC management committee shall:
- 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 risks associated with digital continuity and records management in respect of all data held electronically.

Privacy Statements
BCCC provides a privacy statement to all data subjects, for which we hold data. This is in line with the Information Commissioners Office (ICO) guidance about following GDPR.
Procedures are be in place covering the receipt, storage, correction and deletion of personal, including special category, data. See BCCC's Privicy Policy (incorporating GDP Regulations 2018)

Valuing and Classification Assets
The Contact Centre ensures 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 BCCC will ensure that:

- Information and other assets are valued according to the definitions the classification policy and are clearly and conspicuously marked.
- 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 on the basis of a genuine need to know and an appropriate level of personnel security control;
- Where information is shared for charity purposes BCCC will ensure the receiving party understands the obligations and protects the assets appropriately;

Risk Assessment and Accreditation of ICT Systems

Charity Continuity and Disaster Recovery Plans

- BCCC will ensure that Charity impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications and systems..

- The following arrangement shall be followed:

Risk	Likelihood Score	Mitigation Plan
Loss of staff: As a contact centre many skill sets are very critical to the organisation.	B. High Impact, Low Likelihood.	Capture as much information as possible. Prioritise having volunteers that can cover additional roles.
Loss of premises: e.g. building burns down.	B. High Impact. Low Likelihood.	Rented premises.
Loss of computer	D. High Impact. Low Likelihood.	Back up to USB stick monthly & stored off site.

Reporting

- The Volunteers and Families Coordinator shall keep the trustees and Management Committee informed of the information security status of the organisation by means of regular reporting.

- **Annex A Data Protection Policy**

The Data Protection Act 2018 requires that anyone processing personal data must comply with the enforceable principles of good practice. Birmingham Child Contact Centre will comply with these requirements by ensuring that:

1. BCCC has conducted an information audit to map data flows.

2. BCCC has identified lawful bases for processing and has documented them.

3. BCCC has reviewed how you ask for and record consent.

   NB. "The GDPR sets a high standard for consent but remember you don't always need consent. You should also assess whether another lawful base is more appropriate. Consent to process children's personal data for online services is also required. If your business offers online services directly to children, you communicate privacy information in a way that a child will understand. You must provide children with the same fair processing information as you give adults. It will be good practice to also explain the risks involved in the processing and the safeguards you have put in place."

4. Registered with the Information Commissioners Office, where required

5. To fulfil the obligations to data subjects' right to be informed, everyone will receive a copy of the Privacy Notice. Birmingham Child Contact Centre has a process to recognise and respond to individuals' requests to access their personal data.

   Individuals have the right to obtain:
   confirmation that their data is being processed;
   access to their personal data; and
   other supplementary information – this largely corresponds to the information provided in the privacy notice.

Birmingham Child Contact Centre also has

- processes to ensure that the personal data held remains accurate and up to data,
- a process to securely dispose of personal data that is no longer required or where an individual has asked for it to be erased.
- procedures to respond to an individual's request to restrict the processing of their personal data.
- processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.
- procedures to handle an individual's objection to the processing of their personal data.
- processes to identify, report, manage and resolve any personal data breaches.

These are all included in BCCC's Privacy Policy.