INFORMATION SECURITY POLICY

Reviewed On	February 2022
Next Review Date	February 2024 or when a change to legislation and guidance occurs. This document remains in force after the review date if it has not been replaced.
Related Policies/Procedures	Acceptable Use of IT, Email and Phone Policy
	Confidentiality and Data Protection Policy
	Data Protection Guidance for Staff
	Data Retention & Storage Guidelines
	Information Commissioners Office Guidelines
	Internet, Website and Social Media Policy
Responsible Function	Administration
Version	2022-1
Overview of Changes	Updated Bring Your Own Device section. Image security updated to include voice.

Organisational Responsibilities

The Board of Directors are responsible for the operational management of Colebrook (South West) Limited's policies and procedures.

The Chief Executive Officer (CEO) is the designated officer, on behalf of the Board of Directors, responsible for the implementation of the policies and procedures across Colebrook (South West) Limited.

Contact details

Chief Executive Officer	Vicky Shipway
Telephone Number	01752 205210
E-mail	vshipway@colebrooksw.org

Introduction

This Policy covers Colebrook's approach to managing information security. Colebrook works with a lot of information, some of which is personal or sensitive in nature, so we have a responsibility to:

- Ensure appropriate organisational measures to prevent unlawful processing of personal data
- Ensure only authorised people can access, alter, disclose or destroy personal data
- Prevent information security breaches which can cause harm and distress to individuals and the organisation
- Ensure all staff are trained and aware of their responsibilities
- Work with a layered approach to security which is reviewed regularly
- Comply with the General Data Protection Regulations, Freedom of Information Act, Human Rights Act and Equality Legislation

Scope

This Policy applies to all employees (and potential employees), including those on part-time, apprentice, fixed-term and job-share contracts, as well as other employees and agency staff.

Systems User Access and Controls

Colebrook information is saved on an 'onsite' server, alongside cloud-based systems for email, file sharing and databases (called CharityLog and StaffPlan). Information stored is arranged into defined areas covering

services tasks and sensitive information. Information access to any system is granted dependent on the service area, role and areas of responsibility of each post and is assessed initially at induction and then as needed in response to changes. A designated manager takes the lead in overseeing access across Colebrook, and authorisation to make changes to user access is limited to a small number of identified managers.

Colebrook's IT support is outsourced to a local provider who maintain all IT security, access, backups and can trace and identify activity on our server.

User access on CharityLog is controlled through the use of branches and permissions dependent on whether information is needed and relevant. These vary for different groups of staff and their roles. Access is controlled through a small number of system administrators. Access to CharityLog is achieved through a two-password log in. Passwords are set by Colebrook and individual users, require complexity and are changed regularly.

Staff are trained as part of their induction. When staff leave or move within the organization, access forms part of the exit process and is withdrawn immediately.

IT Security and Backup

Colebrook contracts a reputable IT support solution that covers

1) Server location and security.
2) Antivirus updates to our system with some antimalware protection. Management of cloud-based Firewall.
3) Driver and access management to ensure the system set up allows for staff to access relevant areas
4) Facility to offer encryption software and processes to meet the needs of our services on portable media.
5) Nightly back up of all data held both on site for quick recovery and offsite, stored in a secure data centre.
6) Regular updates to the server and file sharing system.
7) Options for external security audit of access, including a dated log of all access authorisations and changes.

Security audit is also built into internal checks, covering access to equipment, checks on information on desktops and laptops. Colebrook forces password changes on a regular basis.

It is not Colebrook policy to allow the removal of personal information off site. However, staff may need to work remotely on information which is sensitive in nature so memory sticks are encrypted as a matter of course to protect any information saved.

All portable equipment (phones, laptops and tablets), require an initial password access and further individual password access to log remotely onto any of our systems. Phones issued can be remotely wiped if lost or stolen.

'Bring Your Own Device' (BYOD)

See also Use of Personal Phones and Equipment for business Purposes in the Acceptable Use of IT, Email and Phone Policy

Where Colebrook staff are authorised to use their own devices for Colebrook related work, the following applies

- Colebrook remains in control of all data regardless of the device used.
- You must not store any Colebrook documents or data on your own devices. If you need to open a document from email, please ensure it has not saved on the phone.

- Information is accessed through remote access to Colebrook servers or databases via a protected login.
- Staff will ensure there is updated security on their devices; which as a minimum ensures:
  - All devices are protected by passwords which are complex, changed regularly and confidential.
  - All devices are set up to automatically lock after a period of inactive use.
  - All equipment used for connecting to Colebrook systems, viewing Colebrook email or Microsoft Teams or containing a Colebrook SIM must require either password, PIN, pattern, fingerprint or face recognition access and any password, PIN or pattern access must not be known by anyone else, including household members.
- Use of the internet, email or social media will adhere to Colebrook's Policies in these areas.
- Staff will ensure that all information accessed through their own devices is used appropriately as stated in the General Data Protection Regulations.
- Staff must alert their manager immediately if devices used are lost, stolen or no longer in use so that staff access can be changed and updated.
- Any personal devices used to access Colebrook systems or data will be subject to spot check to ensure appropriate protection is in place. Colebrook will hold a log of all 'own' devices used by staff who will sign a checklist to confirm compliance with the policy.

Clear Desk Policy

A clear desk will reduce the risk of unauthorised access or loss of sensitive information; whether the information is on paper, a storage device or on a computer. Shared offices and desks present an information security risk.

When a desk is unoccupied for a period of time, all Colebrook staff will:

1) Lock away all sensitive and confidential information.
2) Log off work stations.
3) Lock portable devices away.
4) Keep keys on their person or secured.
5) Use confidential printing and shredding for relevant information.

Visitors will be supervised and Colebrook staff will be aware of visitors and use the above responses where visitors may have visibility of desks.

Clear desk practice will form part of Colebrook's regular checks. Posters in all offices will be visible to remind staff of their responsibilities.

Image and Voice Security

Colebrook may hold photographs, video recordings or CCTV images of its staff, clients and other stakeholders.

Photographs and video recordings are only taken with permission and where possible photographs and video recordings in public areas are taken so as not to identify anyone accept those who are the focus Consent forms are used for all staff and those clients where photographs and video recordings are taken, to explain their use and gain permission. In the case of staff, some photographs are taken for legitimate use according to GDPR and this is also explained on the consent form.

CCTV images are captured in some properties owned or managed by Colebrook. They are used only to maintain the security and Health and Safety of Colebrook's property, premises, staff and clients. Images may be viewed live to prevent incidents but are more usually recorded for later review should an incident be reported. Images are only captured externally, showing the approaches to buildings, or in communal areas of shared buildings such as offices, corridors, lounges and kitchens. Images are never captured in private areas such as bedrooms or bathrooms. Signage is clearly displayed to inform all people in the area of the cameras that CCTV is in operation. Images are not shared with anyone outside the organisation accept as part of a criminal investigation or prosecution or a Subject Access Request (SAR). In the case of SARs the

information will be viewed first by the CEO or their representative to ensure that no other person's identity could be revealed/compromised by releasing the images, otherwise the request will be refused.

There is clear guidance in the Data Retention Guidance on the maximum length of time photographs and CCTV images will be kept

Colebrook may use voice recording equipment in certain circumstances to record meetings instead of using minute takers. Permission will be gained in writing from all in attendance in advance, or verbally as part of the recording. Copies of the recording can be made available to those present on request. Colebrook's copy will be deleted as soon as minutes are typed up and agreed by all parties, where agreement cannot be reached, this will be noted on the minutes and the recording retained.

Colebrook may record online video meetings. Permission will be gained in writing from all in attendance in advance or verbally as part of the recording. These meetings will be stored on our main server or file sharing platform in an appropriately restricted area for review. If the meeting is turned into written minutes afterwards, the original recording will be deleted.

We may take video recordings for publicity and promotion purposes. Consent forms are used to gain permission from all staff and clients where video is taken to gain permission and explain the intended use.

We recognise that clients and service users are not breaking the law if they record conversations, even without our consent. If we are asked to give consent to being recorded, please discuss with your manager, we will need to look at the reasons for the recording and what it is intended to be used for. We may agree to be recorded if it is intended for personal use. We will never agree to any recordings being provided to third parties or uploaded online through any platform unless they are specifically made for this purpose

Premises Security

Colebrook's main offices require key access, which is held in a key safe outside the main entrance. There is also a security alarm.

Colebrook operates a number of key cabinets that have restricted access and hold keys to properties, general areas, identified offices and areas where personal or sensitive information may be stored. Key access and permissions are held centrally and renewed as needed or with changes.

Colebrook offices situated in projects or centres are accessed by identified staff only holding keys.

Retention, Storage and Archiving

Colebrook has guidelines outlining the type of information that can/should be retained and for how long based on good practice and legal responsibilities. Information may be retained electronically and in paper form in secured filing, accessed by named staff (dependent on the nature of the information).

Current information is archived as people move on from our service, leave our employment or periodically to ensure we are only using current, up to date information. Appropriate information is then archived to secure storage for the appropriate retention period, while remaining information is deleted or destroyed.
Disposal of information happens through

- Confidential shredding by an external provider
- Erasing and destruction of memory sticks, drives
- Shredding of CDs
- Professional recycling of computers and laptops

All staff have the responsibility to audit and check the information they are storing to ensure it is up to date and relevant. Key staff in each service area also have responsibility for overseeing retention and disposal of information and carry out regular audits.

Asset disposal is overseen by an identified user. Organisational information should not be stored on devices, however, to ensure compliance with the Data Protection Act when assets are returned for disposal or reuse, we will

- Ask staff to check and wipe each asset before returning it
- Further check each asset for information saved and delete unnecessary information and personal information before re issue
- Use our current IT provider who works with a specialist disposal service for all hardware

Staff Communication and Training

Information security forms part of

1) Staff induction into the organisation (as part of the induction our Policies and Procedures are read, including signing to confirm they have read all).
2) Team meetings, supervisions and discussions.
3) Mandatory training program (including eLearning).
4) Updates (via email and full staff events).

Data Sharing

We recognise that to deliver our services, Colebrook will need to share and receive data

- Within and across our organisation
- With third parties (on a systematic or ad-hoc basis)

Colebrook uses Privacy Statements to explain how data is held and shared according to and under GDPR, where relevant.

Where there is a need to share systematic information, Colebrook will work with information sharing agreements with third parties to include

- What information will be shared and why?
- Who has access and why?
- Security standards for the data shared for both parties
- Responsibilities of each party
- Retention and deletion of data shared
- Searches for breaches
- Review of the agreement

Where information may be shared on an ad-hoc basis, staff will have access to a checklist to ensure all decisions are based on appropriate and relevant information sharing principles.

Colebrook will respond to individual subject access requests to information held within a timely manner, as per legislation.

Security Breaches

Staff have a responsibility to monitor information security for themselves and others. Staff should immediately challenge or raise with a manager when they are aware of:

1) Personal or sensitive information which is unattended or not locked away.
2) Inappropriate IT access, access to information outside of their role or concerns about access.
3) General concerns about information security.
4) Actions that fall outside of this Policy.

Managers should inform the Central Senior – Administrator of any breach of management, implementation and monitoring of this policy and/or the GDPR. The Central Senior – Administrator will maintain the breaches log.

Where there are concerns or actions in breach of this policy, these will be dealt with internally through our disciplinary procedure and treated very seriously.

Each breach/potential breach will be considered in terms of

1) Severity – What has happened? Is it internal or external? What is the extent of the breach?
2) Containment and recovery – How can the risks be contained? Any procedures for damage limitation?
3) Notification – Who needs to know and why? Individuals? ICO? Regulatory bodies?
4) Evaluation and response – Investigation of causes? Update policy? Staff training?

Implementation, Monitoring and Review of this Policy

The CEO has overall responsibility for implementing and monitoring this Policy, which will be reviewed on a regular basis following its implementation and additionally whenever there are relevant changes in legislation or to our working practices. Any queries or comments about this policy should be addressed to the CEO.