



Policy and Procedure on

Confidentiality Code of Practice

Policy Author / Reviewer	Nicholas Foster
Next Review Date	September 2026
Version No	6
Policy Level	Group
Staff Groups Affected	All Staff

Contents

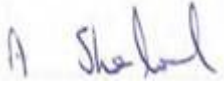
1. Monitoring and Review	1
2. Terminology	2
3. Introduction	2
4. Purpose	4
5. Policy	4
6. Procedures	5
Protection of individual information	6
Conditions relating to disclosure of confidential information	6
Informing Individuals effectively	7
Determining when information may be released	7
What Constitutes Consent	7
Secure Transfer of Information	8
Requesting and Receiving Confidential Information	8
What to do if there is a suspected breach of confidentiality	8
Ensuring quality of information	8
Rights to Access Information	9
Complaints	9

1. Monitoring and Review

- 1.1. The Proprietor will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date of approval shown above, or

earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed:



Amanda Sherlock
Senior Information Risk Owner (SIRO)
Executive Director, Compliance & Regulation
September 2024

2. Terminology

2.1. Our aim is to use consistent terminology throughout this policy and all supporting documentation as follows:

'Establishment' or 'Location'	this is a generic term which means the Children's Home/school/college.
Individual	means any child or young person under the age of 18 or young adult between the ages of 18 and 25 or employee of the Cambian Group.
Service Head / Head of Service	This is the senior person with overall responsibility for the Location.
Key Worker	Members of staff that have special responsibility for Individuals residing at or attending the Establishment.
Parent, Carer, Guardian	means parent or person with Parental Responsibility
Regulatory Authority	Regulatory Authority is the generic term used in this policy to describe the independent regulatory body responsible for inspecting and regulating services.
Social Worker	This means the worker allocated to the child/family. If there is no allocated worker, the Duty Social Worker or Team Manager is responsible.
Placing Authority	Placing Authority means the local authority/agency responsible for placing the child or commissioning the service
Staff	Means full or part-time employees of Cambian, agency workers, bank workers, contract workers and volunteers.

3. Introduction

3.1 This policy deals with the confidentiality code of practice which is to be followed throughout Cambian with regard to the confidentiality of individual and employee information, the confidentiality of commercially sensitive

information relating to Cambian and its operations, and individuals consent to use their health/education records and other information.

3.2 It affects all staff.

3.3 Make sure that you are familiar with the detail and what is expected of you under the policy.

4. Purpose

4.1 The primary purpose of this document is to ensure that Cambian has practical measures in place to ensure that it complies with the Data Protection Act and such extensions to the scope of that act as put forward in the recommendations of the Caldicott Report (1997).

4.2 The objective of this document is to provide everyone who deals with personal or commercially sensitive data with guidelines which will facilitate and guide their actions in respect of treatment of data.

5. Policy

5.1 This code of practice applies to all personally identifiable information, whether in electronic or hard copy form or such as might be disclosed in conversation either with an external party or between Cambian employees

5.2 It also applies to any commercially sensitive information concerning the plans, finances or commercial policies of Cambian.

5.3 The code will provide guidance on the following areas:

- Requirements of a confidential service: Record keeping, Security of information.
- Informing individuals effectively.
- Determining when information may be release and to whom.
- What constitutes consent.
- What to do if there is a breach of confidentiality.

- 5.4 The term Safe Haven is used to define a location (or in some cases a piece of equipment – e.g. fax machine) situated on Cambian premises where arrangements and procedures are in place to ensure personal information can be held, received and communicated securely.
- 5.5 Individual/Personal Information is information which can identify a person – in which the person is the focus of the information and which links that individual to details which would be regarded as private e.g. name and private address, name and home telephone number, NHS number etc.
- 5.6 Special Category Data/Sensitive Personal Information is defined as consisting of information which relates to the individual's: race or ethnic origin, political opinion, religious or other beliefs, trades union membership, physical or mental health or condition, sexual life or criminal proceedings or convictions.
- 5.7 Sensitive Commercial Information is any information relating to Cambian's business or processes which, if compromised (through alteration, corruption, loss, misuse, or unauthorised disclosure), could cause harm to the business.

6. Procedures

- 6.1 **The Senior Information Risk Owner** has overall responsibility for confidentiality and data protection issues.
- 6.2 Primary responsibility for confidentiality of individual information lies with the **group Caldicott Guardian**.
- 6.3 Each Establishment has a nominated **local Caldicott Guardian** who can provide local advice on confidentiality and data protection issues. Each local Guardian should inform the group Caldicott Guardian or the Data Protection Officer of any issues that they are unable to resolve.
- 6.4 The group Caldicott Guardian will work with local Caldicott Guardians, the Data Protection Officer, managers and employees to bring about a culture of awareness of the requirements to manage confidentiality and data protection issues.
- 6.5 **All Cambian employees** have a duty to comply with this policy and with any Data Protection Procedures published by the Group from time to time if, as part of their responsibilities, employees collect information about other people (e.g. about other employees or individuals at their Establishment / Department).
- 6.6 While specific roles are mentioned in this Code of Practice, it is the responsibility of every employee and every consultant or contractor to ensure that the practices identified in this document are adhered to.
- 6.7 Cambian has appointed a group Caldicott Guardian who is charged with responsibility for all matters relating to individual confidentiality. The Responsible Clinicians (Adult Services) and Heads of Establishment (Children Services) have also been appointed as local (or 'site') Caldicott Guardians who are available to assist in resolution of individual confidentiality matters, and who may refer matters to the Group Caldicott Guardian if necessary.
- 6.8 The two key concepts in the code of practice are that:
- Information should only be released if there is an established method of release already in place.
 - If no standard procedure exists, then any request for release of information should be referred to the local Caldicott Guardian, who will provide advice and guidance.

Protection of Individual Information

6.9. Individuals have the right to have their confidential data kept secret from all persons who do not have a direct role in their medical treatment or who are authorised by receive confidential information for their case.

6.10. This means that confidential information should always be securely maintained. Employees must:

- Shut /lock doors and cabinets as required.
- Wear building passes and identification tags as required.
- Query the status of strangers.
- Know who to tell if anything suspicious or worrying is noted.
- NOT tell unauthorised personnel how security systems operate.
- NOT breach security themselves.
- NOT discuss any personal information when it could be overheard by an unauthorised person.
- As a general rule, take particular care and measures to protect sensitive personal data from unauthorised access.

6.11. Manual records must be:

- Booked out from filing systems.
- Tracked if transferred.
- Returned to filing as soon as possible.
- Securely stored where they are not left on view in circumstances in which they could be read by unauthorised persons.

6.12. With electronic records, employees must:

- Exit any applications and log off systems when their work on them is finished.
- NOT leave terminals logged on and unattended.
- NOT position terminals where they are visible to casual observers.
- NOT share logins or sessions with other people.
- NOT reveal passwords in any way.
- Change passwords as required by GIG 07: Information Systems AUP.
- Clear one individual's data from screens before seeing another individual.

Conditions relating to disclosure of confidential information

6.13. Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given. Information may only be disclosed under conditions of certainty regarding who may have access to the data. In particular employees must:

- Follow any specific procedures and protocols relating to particular systems, information or individuals.
- Ascertain with certainty that the person to whom they are disclosing data is a person authorised to receive the data and are who they claim to be.
- For requests by phone, identify the person's name, job title and organisation. Then separately identify the phone number of the organisation and then ring the reception/switchboard and ask to be put through to the person.
- For personal requests, proof of identity should be requested.
- Personal data should only be disclosed to Police Officers if they are able to supply formal, written confirmation of a specific, legitimate need to have access to specific personal data.
- Ensure that when transmitting data, that it will be received in a secure manner consistent with the requirements of confidentiality (e.g. Safe Haven).

- Disclose the minimum amount of information required commensurate with the desired outcome.

6.14. If there is any ambiguity as to whether information should be disclosed, then DO NOT disclose the information, but refer the matter to the Data Protection Officer, local or group Caldicott Guardian. For all disclosures of personal information, a record should be made so that the recipient can be informed if the data is later found to be inaccurate.

Informing Individuals effectively

6.15. All individuals who are the subject of personal data held by the Group are entitled to:

- Ask what information the Group holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed what the Group is doing to comply with its obligations under the Data Protection Act.

6.16. Individuals should be informed clearly and unambiguously that information which they give will be recorded and may be shared to provide them with care/education services and to support audit of those services.

6.17. The following points must be considered in respect of ensuring that individuals are informed properly about treatment of their confidential information:

- Ensure individuals have seen relevant information leaflets explaining to them what their information is to be used for.
- Make it clear that they understand the choices they have with respect to disclosure, including the right to specify who may not receive their information.
- Ensure they have no unresolved concerns or queries.
- Ensure they understand that they have the right of access to their records.

Determining when information may be released

6.18. The diagram in GIG 09.1 shows the flow of decisions and steps that should be undertaken prior to release of confidential information.

What Constitutes Consent

6.19. Consent is: *“any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”*. Therefore, if the individual has no real choice, consent is not freely given and it will be invalid.

6.20 The Group will only obtain an individual’s consent where there is genuine choice and genuine control by the individual whether or not to consent to the processing of their personal information. We will rely on other legal bases where they are appropriate for the processing. Advice should be sought from the Data Protection Officer, local or group Caldicott Guardian as required.

6.21. The following points should be noted where consent is required:-

- Consent must be obtained from any individual competent or able to do so.
- Explicit consent should be obtained from a individual in a manner which:
 - Is honest and objective about the use of data.
- Allows time for individuals to consider and if necessary discuss their decision.
 - Provides any explanations requested regarding forms to be signed.
 - Allows individuals to reconsider regarding future choices and future methods of contact regarding consent.
 - Advise the individual that they can withdraw their consent at any point.

- Provides evidence that consent has been given.
- Individuals have the right to withhold consent to disclosure of information provided in confidence in a form which makes them identifiable. When the individual is competent to make such a decision and is aware of the consequences, then the information should not be disclosed.

Secure Transfer of Information

6.22. All Cambian employees have a duty to ensure that personal or sensitive information sent to an external party is secured in transit. In practice this means that once the requesting person has been confirmed as being authorised to receive the information:

- Any information sent via post must be sent by recorded delivery or courier service to a named individual. The package should be marked "Private & Confidential" and the Sender's details are clearly identifiable.
- If the information is to be sent by fax, the person requesting the information needs to confirm that the receiving fax machine is in a secure 'Safe Haven' location.
- Any confidential information sent by email to external parties should be sent only once 2 way confirmation of the intended recipients has been authenticated in advance. Any confidential or Personal Identifiable Information is to be sent encrypted by an appropriate encryption tool (e.g. 3rd Party Encryption or Egress Switch,). Should none of these tools be available then at a minimum data should be password protected using the built in security measures available in Adobe PDF or Microsoft Applications.

Requesting and Receiving Confidential Information

6.23. In circumstances where Cambian employees need to request personal or sensitive information, the requirements identified above must apply in reverse. i.e.:

- If the information is to be posted, then employees must provide specific recipient details such that the post will be opened in a secure area.
- If the information is to be faxed, then employees must confirm that the Cambian fax machine is located in a secure area. If the information is to be e-mailed, once 2 way email authentication is complete, then employees should request that the information is sent in a password protected zip file.

6.24. As a general principle, wherever possible, it is good practise to 'anonymise' the information by the removal of any details that may support identification of the individual (e.g. by the use of an agreed individual identifier).

What to do if there is a suspected breach of confidentiality

6.25. If employees identify a possible breach of confidentiality, then they must raise their concerns initially with their manager, the local Caldicott Guardian who should then report the matter to the Data Protection Officer.

Ensuring quality of information

6.26. Employees must:-

- Check that any personal data that they provide to the Group is accurate and up to date.
- Inform the Group of any changes to information which they have provided, e.g. changes of address.
- Check any information that the Group may send out from time to time, giving details of information that is being kept and processed.
- Inform their Head of Establishment or function of any errors in the information held by it relating to them or to individuals.

Rights to Access Information

6.27. Employees and other subjects of personal data held by the Group have the right to access any personal data that is being kept about them on computer and also have access to paper-based data held in certain manual filing systems. This right is subject to certain exemptions which are set out in the Data Protection Act. Any person who wishes to exercise this right should make the request, in writing, to the Group Data Protection Officer [GIG 08 Access to Records](#).

Complaints

6.30. Any employee who considers that the policy has not been followed in respect of personal data about themselves should, in the first instance, raise the matter with their Line Manager who should, in turn, consult the Head of their Establishment or Department. If the matter then remains unresolved it should be raised as a formal grievance using the Group's Grievance Procedure (GHR 25). Heads and Managers of departments should upon receipt of any grievance relating to a failure to observe this Policy, or any query concerning it, consult with Human Resources.