Policy No:
GIG 02.00

Policy and Procedure on

Data Protection

Policy Author / Reviewer	Paul Follan/ Greg Regan
Approval Date	September 2018
Next Review Date	September 2019
Version No	2
Policy Level	Group
Staff Groups Affected	All Staff

Contents

1. Monitoring and Review

11. 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 two years 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:

Anne Marie Carrie
Proprietor, Cambian Group
May 2016

Greg Regan
Interim Principal
September 2018

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.
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 principles and the attendant procedures of Data Protection as it applies to all the appropriate activities throughout the Group and its Locations.

3.2. This policy has been approved by and applies to Cambian Capital Limited and its direct and indirect subsidiaries and Care Aspirations Capital Limited and its direct and indirect subsidiaries and references to the "Cambian Group" shall be construed as referring to all such companies.

3.3. Its affects all staff.

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

4. Purpose

4.1. To ensure that Cambian Group complies with all the relevant current legislation and other National Standards which govern this area of our work.

4.2. To recognise the importance of the correct and lawful treatment of personal data; to maintain confidence in the Group and to provide for successful operations.

5. Policy

5.1. The Cambian Group shall maintain, as required, certain personal data about living individuals for the purposes of satisfying operational requirements and legal obligations.

5.2. The types of personal data that the Group may hold includes information about:

- current, past and prospective employees;
- current, past and prospective students and residents;
- individual staff members of placing authorities;
- individual staff members of suppliers and others with whom it communicates.

5.3. This personal data, whether it is held on paper, on computer or other media, shall be subject to the appropriate legal safeguards as specified in the Data Protection Act 1998.

5.4. The Cambian Group fully endorses and adheres to the eight principles of the Data Protection Act. These principles specify the legal conditions that must be satisfied in relation to obtaining, handling, processing, transportation and storage of personal data. The Group will retain its data and records in accordance with the requirements of ISO 9001/2008 and other appropriate Regulations and Standards.

5.5. The Cambian Group have Data Protection Officers to ensure the Group meets its operational and legal obligations. A list of Data Protection Officers can be found in each Location. Employees and any others who obtain, handle, process, transport and store personal data for the Group shall adhere to these principles:

Principles

5.6. The principles require that personal data shall:

- be processed fairly and lawfully and shall not be processed unless certain conditions are met;
- be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- be adequate, relevant and not excessive for those purposes;
- be accurate and, where necessary, kept up to date;
- not be kept for longer than is necessary for that purpose;
- be processed in accordance with the data subject's rights;
- be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures;
- and not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Satisfaction of principles

5.7. In order to meet the requirements of the principles, the Group shall:

- observe fully the conditions regarding the fair collection and use of personal data;
- meet its obligations to specify the purposes for which personal data is used;
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements;
- ensure the quality of personal data used;
- apply strict checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act;
- take the appropriate technical and organizational security measures to safeguard personal data;
- ensure that personal data is not transferred abroad to countries without suitable safeguards in place.

The Group's Designated Data Protection Officers

5.8. It is the Group's policy to maintain, via the Group's Company Secretary and Head of Legal, registration of each of its operating companies, Cambian Care Services Limited, Cambian Healthcare Limited, Cambian Autism Services Limited, Cambian Asperger Syndrome Services Limited, Cambian Education Services Limited, Cambian Learning Disabilities Midlands Limited, Cambian Learning Disabilities Limited, Cambian Learning Disabilities Services Limited, Cambian Ansel Limited, Cambian Childcare Limited, Cambian Whinfell School Limited, By The Bridge Limited, By The Bridge North West Limited, with the Office of the Information Commissioner.

5.9. Each of those companies is the data controller in respect of the data processed by it. The named contact for each company is the Group's Company Secretary and Head of Legal, who is ultimately responsible for ensuring compliance with the Data Protection Act and implementation of this policy on behalf of the Board. Any questions or concerns about the interpretation or operation of this policy should be taken up, in the first instance, with the Company Secretary.

Status of the Policy

5.10. This policy has been approved by the Board and any breach will be taken seriously and may result in formal disciplinary action.

6. Procedures

Subject access

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

- ask what information the Group holds about them, the source of the data and purpose of holding it;
- Gain access to it.

Employee Responsibilities

6.2. All employees are responsible for:

- ensuring that any personal data that they provide to the Group is accurate and up to date;
- informing the Group of any changes to personal information which they have provided, e.g. changes of address;
- informing the Group of any errors in the information held by it relating to them;
- complying 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 in our care at their Location, department or house unit).

Data Security

6.3. The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage and that both access and disclosure must be restricted.

6.4. All staff are responsible for ensuring that:

- any personal data which they have access to is kept securely;
- personal information is not disclosed either orally or in writing or otherwise to any unauthorised third party;
- computer workstations in administrative areas are positioned so that they are not visible to casual observers and are not left unattended when the user is still logged-on or in any other circumstances when the personal details of staff or individuals in our care could be accessed by unauthorised persons;
- papers containing personal information are stored where they are not accessible to anyone who does not have legitimate reason to view or process them and they are not left on view in circumstances in which they could be read by unauthorised persons;
- particular care and measures are taken to protect sensitive personal data from unauthorised access.

- Cambian will identify Data Owners for specific types of data stored at both local and core level. These Data Owners are ultimately responsible in conjunction with IT Staff for ensuring that data is restricted internally to only those individuals or groups of persons who need access to any data through the course of their work role.

Right to Access Information

6.5. 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 electronically 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 Human Resource Director. [NB The Policy on Confidentiality – Code of Practice IT 2.6 says the Group Data Protection Lead deals with SARs?]

6.6. The Group reserves the right to charge the maximum fee payable for each subject access request. If personal details are inaccurate, they can be amended upon request.

6.7. The Group will endeavour to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of a request unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the individual making the request.

6.8. The Group reserves the right to charge a payable fee from legitimate 3rd party requests for information when the resource required to provide that information is labour intensive (e.g. photocopying large Service User Records, collection of electronic data. Each request should be reviewed and guidance sought from the Caldicott Guardian or Company Secretary in the event that the request warrants a payable fee being raised.

Data Disclosures

6.9. Personal data will only be disclosed to organisations or individuals for whom the data subject's consent has been given, or organisations that have a legal right to receive the data without consent being given.

6.10. When requests to disclose personal data are received by telephone it is the responsibility of the Location to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

6.11. If a request is made in person for personal data to be disclosed it is the responsibility of the Location to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

6.12. Personal data or photographs will not be used in newsletters, websites or other media without the consent of the data subject.

6.13. Routine consents will be incorporated into the Location's individuals in our care data gathering sheets to avoid the need for frequent, similar requests for consent being made by the Location.

6.14. Personal data should only be disclosed to Police Officers if they are able to supply formal, specific written confirmation of a specific, legitimate need to have access to specific personal data e.g. to assist in criminal investigations.

6.15. A record should be kept of any personal data disclosed as an audit trail and so that the recipient can be informed if the data is later found to be inaccurate.

Subject Consent

6.16. The need to process data for the Group's operational purposes should be communicated to all data subjects.

6.17. In some cases, if the data is sensitive, for example information about health, race or gender, express consent to process the data must be obtained. Processing may be necessary to operate Group policies such as 'Health and Safety' and 'Equal Opportunities'.

Publication of Cambian Group Information

6.18. Consent will not be required to publish information already in the public domain. This would include, for example, information on staff contained within externally circulated publications such as the Cambian Bulletin and Locations' Parent Newsletters. Any individual who wishes to withdraw their consent to their data being circulated in such publications should contact the Human Resource Director.

Complaints

6.19. Any employee who considers that this 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 Location or Department. If the matter then remains unresolved it should be raised as a formal grievance using the Group's Grievance Procedure (HR). Heads/Hospital Managers and Managers of departments where there is no Head should upon receipt of any grievance relating to a failure to observe this Policy, or any query concerning it, consult with the Human Resource Director.

Retention of Data

6.20. The Group needs to retain information whilst service users and employees remain looked after or employed by it and for a period after the relationship terminates in accordance with statutory limitation periods. All staff are responsible for ensuring that information is not kept for longer than necessary.

6.21. This policy should be read in conjunction with the Group Policy: The General Use of IT in Group Locations. Further information and guidance is available on the Information Commissioners website www.dataprotection.gov.uk

6.22. All employees managing and handling personal information will be appropriately trained and supervised. All enquiries about the handling of personal information will be dealt with promptly and courteously.

6.23. A regular review will be undertaken of the way in which personal information is managed.

7. Standard Forms, Letters and Relevant Documents

7.1. GIG 09 – Confidentiality Code of Practice

7.2. GIG 02.1 – Appendix 1 – Acts of Parliament Relevant to release of Information