Cambian

Policy and Procedure on

Data Protection

Policy Author / Reviewer	Nicholas Foster
Approval Date	July 2018
Next Review Date	July 2020
Version No	3
Policy Level	Group
Staff Groups Affected	All Staff

Contents

1. **Monitoring and Review** 2
2. **Terminology** 2
3. **Introduction** 4
   Status of the Policy 4
4. **Purpose** 4
5. **Policy** 4
   Principles 5
6. **The Group's Data Protection Officer** 5
7. **Notifying the Data Protection Officer of certain activities** 6
8. **Employee Responsibilities** 6
9. **The lawful bases for processing personal information** 7
10. **Criminal Convictions Data** 7
11. **Data Subject's consent** 8
12. **Children** 8
13. **Direct Marketing** 8
14. **Data security and Retention** 9
    Retention of Data 9
15. **Right to Access Information** 9
16. **Data Disclosures** 10
17. **Transferring Personal Information outside of the European Union** 10
18. **Personal Information Breach** 10

® Cambian Group PLC 2014

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 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
July 2018

2. Terminology

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

Personal Information/ Personal Data	Personal information is any information about any living person from which they can be identified. This can be on paper, on a computer or even just talked about. Personal information can relate to, for example, past or present employees/workers, contractor/ suppliers, customers or shareholders. Some examples are: personal contact details, such as name, address, email, telephone number, date of birth, bank account details.
Special Category of personal information/Sensitive Personal Information	Information about an individual's racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; health; sex life or sexual orientation; criminal convictions, offences or alleged offences; genetic data; or biometric data for the purpose of uniquely identifying an individual.
Processing	Any activity that involves using personal information. This includes collecting personal information, recording it, storing it, retrieving it, using it, amending it, disclosing it, destroying it, and transferring it to third parties.

Data Protection Impact Assessment	A data protection impact assessment is an assessment of the impact of the envisaged processing operations on the protection of personal data.
Direct Marketing	Direct marketing means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.
'Establishment' or 'Location'	This is a generic term which means the Children's Home/school/college
Individual/Data Subject	This means the person whose personal information is held by 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.

® Cambian Group PLC 2014

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 Cambian Group and its Locations.

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

3.3. It affects all staff and must be read in conjunction with the following policies:

- Information Security (GIG 04)
- Risk Management (GIG 05)
- Records Management (GIG 06)
- Information Systems Acceptable Use (GIG 07)
- Access to Records (GIG 08)
- Confidentiality Code of Practice (GIG 09)

3.4. All employees should make sure that they are familiar with the detail and what is expected of them under these policies.

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

Status of the Policy

3.6. This policy has been approved by the Serious Information Risk Officer and any breach will be taken seriously and may result in formal disciplinary action.

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 need to process data for the Group's operational purposes should be communicated to all data subjects. Further information of the Group's operational purposes and how it handles personal data is outlined in the Privacy Policy which is available on the website at this location: http://www.cambiangroup.com/cambiangroup/privacypolicy.aspx

5.3. 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;

- Shareholders, foster parents and others with whom it communicates.

5.4. 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 General Data Protection Regulations 2016 (GDPR) and Data Protection Act 2018.

5.5. The Cambian Group fully endorses and adheres to the six 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.

5.6. The Cambian Group have a Data Protection Officer and Data Protection Champions to ensure the Group meets its operational and legal obligations. Details of the Data Protection Champion 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

5.7. The principles require that personal information must be:

a) Processed lawfully, fairly and in a transparent manner;
b) Collected only for specified, explicit and legitimate purposes, and processed only in line with those purposes;
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d) Accurate and, where necessary, kept up to date;
e) Not kept in a form which permits identification of individuals for longer than necessary, in relation to the purposes for which it is processed;
f) Kept secure, and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Satisfaction of principles

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

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

6. The Group's Data Protection Officer

6.1. 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 Group Plc, Cambian Group Holdings Limited, Cambian Signpost Limited, Cambian Autism Services Limited, Cambian Asperger Syndrome Services Limited, Cambian Education 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.

6.2. 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 together with the Data Protection Officer, 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 Data Protection Officer.

7. Notifying the Data Protection Officer of certain activities

7.1. It may be necessary for Data Protection Officer to carry out a 'data protection impact assessment' before you undertake certain activities that involve processing personal information.

7.2. A 'data protection impact assessment' will consider the impact of the activities; identify privacy risks and steps to minimise those risks; and evaluate whether the activities are permitted by data protection law. As such, employees should seek advice from the Data Protection Officer so they can advise whether a data protection impact assessment is required in the following situations:

a) Process new types of personal information i.e. personal information which has not been collected before.
b) Process personal information in a new or significantly different way, including via the use of new technologies.
c) Use personal information for a purpose other than that for which it was collected.
d) Enter a contract with a third party that involves disclosing or sharing personal information.
e) Any new or significantly different use of automated processing of personal information to evaluate an individual, for example to analyse or predict an individual's performance at work, health, personal preferences, interests, reliability, behaviour, location or movements.
f) Any new or significantly different use of automated decision-making i.e. where a decision is made on a solely automated basis without meaningful human involvement, and it has a significant effect on individuals.
g) Any new or significantly different large scale processing of special categories of personal information; or large scale, systematic monitoring of a publicly accessible area. Whether processing is 'large scale' will depend on, for example, the number of individuals, volume of data, range of data, duration of processing, or geographical extent – if you are in any doubt as to whether processing is large scale, contact the Data Protection Officer.
h) Implement significant changes to systems or the business (including new or different technology) which involve processing personal information.
i) Any new direct marketing activity (including electronic marketing by email, telephone, fax or text message).
j) Transmit or send personal information to, or view or access personal information in, a country outside of the European Economic Area (EEA), where this has not been previously authorised by the Data Protection Officer or in line with the Group's Data Protection Policy. The EEA is the 28 countries in the European Union, along with Iceland, Liechtenstein and Norway.

7.3. Employees must comply with any directions from the Data Protection Officer in relation to the above, and the terms of any data protection impact assessment.

8. Employee Responsibilities

8.1. 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).

8.2. All employees managing and handling personal information must complete the mandatory Information Governance modules, which includes data protection.

9. The lawful bases for processing personal information

9.1. The Group will only process personal data where it is strictly necessary to carry out a specific purpose. The processing of personal data must be based on one of the legal bases listed below:

a) the data subject has given his or her consent.
b) the processing is necessary for the performance of a contract with the data subject (e.g. monitoring performance of employees in line with the contract of employment) or where the data subject has requested the Group to take specific steps before entering into a contract (e.g. obtaining employment references from a previous employer).
c) to meet our legal compliance obligations (safeguarding children, for example).
d) to protect the data subject's vital interests (i.e. matters of life or death).
e) to perform a task in the public interest or for our official functions where the task or function has a clear basis in law.
f) to pursue our legitimate business interests providing there is no conflict with the data subjects rights.

9.2. The processing of sensitive personal data represents a greater intrusion in individual privacy than when processing non-sensitive personal data. We will therefore take special care when processing sensitive personal data, in particular in ensuring the necessity of the processing and security of the sensitive personal data. The processing of sensitive personal data must be based on one of the above legal bases for processing non-sensitive personal data as well as one of the additional legal bases below for processing sensitive personal data.

a) The data subject has given explicit consent.
b) The processing is necessary in the context of employment law, or laws relating to social security and social protection.
c) The processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent.
d) The processing is carried out in the course of the legitimate business activities.
e) The processing relates to personal data which have been manifestly made public by the data subject.
f) The processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity.
g) The processing is necessary for reasons of substantial public interest**,** and occurs on the basis of a law, it is proportionate to the aim pursued and protects the rights of data subjects.
h) The processing is required for the purpose of medical treatment undertaken by health professionals**,** including assessing the working capacity of employees and the management of health or social care systems and services**.**
i) The processing is necessary for reasons of public interest in the area of public health.
j) The processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards for the rights of the data subject.

10. Criminal Convictions Data

10.1. There are specific rules regarding the processing of data relating to criminal convictions and offences. Therefore, advice should be sought from the Data Protection Officer or Head of Legal when processing this type of information. Some of the situations where personal data relating to criminal convictions and offences may be processed, are listed below:

a) The data subject has given consent to the processing.
b) The processing is necessary to protect the vital interests of an individual and the data subject is physically or legally incapable of giving consent.
c) The processing is necessary in connection with employment, health or social care, social security or social protection.
d) In order to protect children or individuals from neglect, physical, mental or emotional harm.

e) The processing is necessary to prevent fraud, preventing or detecting unlawful acts.

Data Subject's consent

11.1 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".

11.2. Consent means giving people genuine choice and control over how we use their data. If the individual has no real choice, consent is not freely given and it will be invalid. This means people must be able to refuse consent without detriment, and must be able to withdraw consent easily at any time. It also means consent should be separated from other terms and conditions (including giving separate consent options for different types of processing) wherever possible.

11.3 Whilst consent is one of the legal bases for processing of personal information, it is not required where another legal basis exists. Where consent is required, the data subject must be informed and their wishes must be respected and written record must be retained for auditing purposes.

11.4 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.

11.5. Personal data or photographs will not be used in newsletters, websites or other media without the consent of the data subject. We will seek consent before displaying within our Locations, personal information about individuals (including, certificates/qualifications). Routine consents will be incorporated into the Location's individual's care data gathering sheets to avoid the need for frequent, similar requests for consent being made by the Location.

11.6. 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 employee who wishes to withdraw their consent to their data being circulated in such publications should contact the Human Resource Director.

11. Children

12.1. Communication aimed towards children and young people must be clear and concise. It should be age-appropriate and presented in a way that appeals to a young audience.

12.2. Where we rely on consent as the lawful basis for processing information about children and young people we will ensure that we obtain consent from children aged 13 years and over. For children under this age we will seek consent from whoever holds parental responsibility for the child.

12.3. Where parents have separated or the young person lacks the capacity to consent, consideration should be given to the 'best interests' of the child/young person.

12. Direct Marketing

13.1. Direct marketing" means the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

13.2. The Group will not participate in direct marketing practices in the absence of:

- Explicit consent from the data subject
- A legitimate business interest reason (advice must be sought from the Data Protection Champion at the site or the Group's Data Protection Officer)

13.3. Even where legitimate interests or explicit consent has been established, all correspondence and the relevant webpages/emails must include opt-out options.

13.4. All individuals must be given the opportunity to opt-in to receive material at the point of data collection. The appropriate opt-in mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

13. Data security and Retention

14.1. 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.

14.2. 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 information from unauthorised access.

14.3 Data Protection Champions 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.

Retention of Data

14.4. 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 and the Group's Data Retention Schedule. All staff are responsible for ensuring that information is not kept for longer than necessary.

14. Right to Access Information

15.1. 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.

15.2. All individuals who are the subject of personal data held by the Group are also (in some circumstances) entitled to:

a) The right to be informed about the information we collect about them and how we handle it
b) The right of access to their personal information
c) The right to rectification of their personal information
d) The right to erasure of their personal information
e) The right to restrict processing of their personal information
f) The right to transfer their personal information to another person or organisation
g) The right to object to processing of their personal information
h) The right not to be the subject of any automated decision-making by us using their personal information or profiling them

15.3 These rights are subject to certain exemptions which are set out in the General Data Protection Regulations and Data Protection Act 2018. Therefore, requests from individuals regarding their personal information must be handled in line with the Access to Records policy (GIG 08); and advice must be sought from the Data Protection Champion at the Site or the Group's Data Protection Officer.

15.4. All enquiries about the handling of personal information will be dealt with promptly and courteously.

15. Data Disclosures

16.1. 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.

16.2. 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.

16.3. 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.

16.4. 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.

16.5. 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.

16. Transferring Personal Information outside of the European Union

17.1. There are strict guidelines regarding the sharing of information outside of the European Economic Area (EEA).

17.2. Advice must be sought from the Data Protection Officer before transferring the personal information of any individual to another country.

17. Personal Information Breach

18.1. A personal information breach is a breach of security leading to the accidental or unlawful destruction of personal information; loss, alteration, unauthorised disclosure, or access to personal information transmitted, stored or otherwise processed.

18.2. If you know or suspect that there has been a personal information breach, you must report it immediately to the Data Protection Champion at the Location and the Data Protection Officer. You must also take action to stop the breach getting worse, for example, by:

a) Confirming that an email has been deleted by the recipient following accidental disclosure, or if possible, revoke any further access.
b) Recovering lost paper records or any lost device left in a public place.
c) Changing the access codes to any compromised building.
d) Informing IT in the event of any compromised computer or data access or anything suspicious or untoward on your device, applications or network files + Folders.
e) Disconnecting your device from the network and report directly to IT, if you suspect you are being directly targeted in a cyber-attack.