



CHRYsalis GROUP & SUBSIDIARIES

Chrysalis Group Services Limited
Touchstone Developments & Investments Ltd
Chrysalis Supported Housing Limited
Opoka Charitable Incorporated Organisation
Compass Project CIC
Blackfields Furniture Ltd

INFORMATION GOVERNANCE & RECORD KEEPING (DATA PROTECTION) POLICY

Contents

1.	Introduction.....	3
2	Policy Statement	3
3	Scope	4
4	Roles and Responsibilities	4
5	Definitions.....	5
6	Legislation and Guidance	7
7	The Data Protection Principles	7
8	The Rights of Data Subjects	8
9	Lawful, Fair, and Transparent Data Processing	8
10	Consent	9
11	Specified, Explicit, and Legitimate Purposes.....	10
12	Adequate, Relevant, and Limited Data Processing	10
13	Accuracy of Data and Keeping Data Up-to-Date.....	10
14	Data Retention	11
15	Secure Processing	11
16	Data Protection Impact Assessments and Privacy by Design	11
17	Keeping Data Subjects Informed	12
18	Data Subject Access	13
19	Rectification of Personal Data.....	13
20	Erasure of Personal Data.....	14
21	Restriction of Personal Data Processing	14
22	Objections to Personal Data Processing	14
23	Data Security - Transferring Personal Data and Communications	14
24	Data Security - Storage.....	15
25	Data Security - Disposal.....	15
26	Data Security - Cease of Trade	16
27	Data Security - Use of Personal Data.....	16
28	Disclosure of Data	16
29	Use of Third Parties to Manage/ Disclosing Data to Third Parties.....	16
30	Secondary Uses of Data	17
31	Security of Information	17
32	Data Security - IT Security	18
33	Organisational Measures	18
34	Record Keeping.....	19
35	Freedom of Information.....	20
36	Accountability and Record-Keeping.....	20
37	Transferring Personal Data to a Country Outside the UK	21

Within the Group, there is:

- A private Non-Profit Registered Social Landlord (RSL), regulated and registered by the Regulator of Social Housing and the Financial Conduct Authority, providing specialist supported homes and related services to vulnerable people across England & Wales.
- A Charitable Incorporated Organisation (CIO), Opoka, regulated and registered by the Charities Commission, that supports Polish women and children escaping domestic abuse, helping them establish their recoveries and build new lives free from the threat of abuse.
- A Community Interest Company (CIC), The Compass Project 2012, an addiction recovery-driven project offering a range of support services, providing a pragmatic solution to those recovering from addiction by giving direct interpersonal peer mentorship, counselling, group support, and structured supported homes, alongside a variety of work and retail-based training opportunities.
- A specialist commercial investment, consultancy and property management company, Touchstone Development & Investments Ltd, that supports the wider strategy and property management requirements of the Group.
- A commercial cabinetry and furniture manufacturing company, Blackfields Furniture, offering both internal and external services, adding value within the group.

It is therefore essential that the Governance Framework used within the Group is fit for all of the entities and their stakeholders, recognising the regulatory requirements and specific needs of each organisation within the group. It is also essential that, as service users may access services of more than one organisation within the group, policies and procedures, wherever possible, are consistently applied across the group, that staff are trained using the same guidelines, and that proper information sharing protocols are in place.

For this reason, it has been agreed that all governance-based policies are group-wide but will apply to all entities within the group to meet our mission:

To safeguard and promote the well-being of our service users and communities across the UK, providing appropriately designed high-quality, good-value, sustainable services and homes, demonstrating that all activities through the group can underpin our commitment to deliver for social good whilst being underpinned by a sound commercial ethos.

1. Introduction

- 1.1 The purpose of Information Governance is to give assurance to data subjects, including employees, individuals and service users that their personal information is dealt with in a legal and secure way. If data is stored effectively the best possible care can be provided.
- 1.2 Chrysalis Group ("The Group") recognises the importance of effectively managing information across the business
- 1.3 The Group will use appropriate policies, procedures, management accountability and structures as part of our information governance framework.

2 Policy Statement

- 2.1 It is the responsibility of all employees to follow this policy.
- 2.2 The Group will ensure that all employees are aware of this policy and receive adequate training in information governance.

- 2.3 Information Governance training will be classified as a statutory requirement as part of the employee induction programme.
- 2.4 All new team starters will receive information governance training relevant to their role, as soon as employment is commenced. The training will be annual and guidance and support on this subject will be available to all employees if needed.

3 Scope

- 3.1 The Group is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.
- 3.2 This policy applies to all Group Employees and to all personal data processed by the company relating to any identifiable living person.
- 3.3 For the purposes of this policy, The Group considers itself to be a data controller in respect of all team members and service users. Data processor: acts on behalf of and only on the instructions of the relevant controller. For the purposes of this policy The Group considers that they are the data processor in relation to the service delivered to its service users.

4 Roles and Responsibilities

4.1 Employees

- 4.1.1 Many employees handle information in one form or another. Employees who in the course of their work create, use, or otherwise process information have a duty to keep up to date with and adhere to, relevant legislation, case law and national guidance.
- 4.1.2 All employees of The Group, whether permanent, temporary, or contracted are responsible for ensuring that they are aware of their responsibilities in respect of Information Governance.

4.2 Directors

The directors have overall responsibility for information governance within the company. The Group Company Secretary is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity.

4.3 Senior Information Risk Owner (SIRO)

- 4.1.2 The role of Senior Information Risk Owner (SIRO) in the company has been assigned to the Group CEO. The SIRO is responsible for leading on Information Risk and for overseeing the development of this policy.
- 4.1.3 The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk.

4.4 Caldicott Guardian

- 4.4.1 The Caldicott Guardian has responsibilities for protecting the confidentiality of service-user's information and enabling appropriate information sharing.
- 4.4.2 Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

4.5 Data Protection Officer (DPO)

- 4.5.1 The Data Protection Officer (DPO) will lead on all matters pertaining to Information Governance. The DPO will maintain the confidence of service users, employees and the public, through advice and guidance on the creation of robust and effective mechanisms and assurance processes to protect and appropriately handle data.
- 4.5.2 This includes ensuring that the company is fully compliant with all information governance related legislation and that the company meets statutory and mandatory obligations through development of strategy and implementation of Information Governance policies.
- 4.5.3 The Group Company Secretary is the company's Data Protection Officer with any questions relating to this Policy or to Data Protection Law should be referred to the Group Company Secretary. In particular, the Group Company Secretary should always be consulted in the following cases:
 - a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;
 - b) if consent is being relied upon in order to collect, hold, and/or process personal data;
 - c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;
 - d) if any new or amended privacy notices or similar privacy-related documentation are required;
 - e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
 - f) if a personal data breach (suspected or actual) has occurred;
 - g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
 - h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);
 - i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;
 - j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;
 - k) when personal data is to be used for purposes different to those for which it was originally collected;
 - l) if any automated processing, including profiling or automated decision-making, is to be carried out; or
 - m) if any assistance is required in complying with the law applicable to direct marketing.

5 Definitions

"consent"	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject's
------------------	--

	wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
“data controller”	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, The Group is the data controller of all personal data relating to staff, customers, service users, tenants and agencies used in our business for our commercial purposes;
“Data Protection Legislation”	Means all applicable data protection and privacy laws including, but not limited to, the UK GDPR, the Data Protection Act 2018, and any other applicable national laws, regulations, and secondary legislation in England and Wales concerning the processing of personal data or the privacy of electronic communications, as amended, replace, or updated from time to time.
“data processor”	means a natural or legal person or organisation which processes personal data on behalf of a data controller;
“data subject”	means a living, identified, or identifiable natural person about whom The Group holds personal data;
“EEA”	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
“personal data”	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject;
“personal data breach”	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
“processing”	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

	otherwise making available, alignment or combination, restriction, erasure or destruction;
“pseudonymisation”	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
“special category personal data”	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual orientation, biometric, or genetic data. +gender?

6 Legislation and Guidance

- Data Protection Act 2018
- Freedom of Information Act 2000
- UK General Data Protection Regulation
- Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003
- Private and Voluntary Health Care (England) Regulations 2001
- The Information Governance Review (publishing.service.gov.uk)
- UK GDPR guidance and resources | ICO
- [information-security-policy-v4.0.pdf](https://www.england.nhs.uk/information-security-policy-v4.0.pdf) (england.nhs.uk)
- The Private and Voluntary Health Care (England) Regulations 2001 (legislation.gov.uk)
- Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)

7 The Data Protection Principles

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

- 7.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- 7.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 7.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 7.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;

- 7.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject;
- 7.6 processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

8 The Rights of Data Subjects

The UK GDPR sets out the following key rights applicable to data subjects:

- 8.1 The right to be informed;
- 8.2 the right of access;
- 8.3 the right to rectification;
- 8.4 the right to erasure (also known as the 'right to be forgotten');
- 8.5 the right to restrict processing;
- 8.6 the right to data portability;
- 8.7 the right to object; and
- 8.8 rights with respect to automated decision-making and profiling

9 Lawful, Fair, and Transparent Data Processing

- 9.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:
 - 9.1.1 the data subject has given consent to the processing of their personal data for one or more specific purposes;
 - 9.1.2 the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
 - 9.1.3 the processing is necessary for compliance with a legal obligation to which the data controller is subject;
 - 9.1.4 the processing is necessary to protect the vital interests of the data subject or of another natural person;
 - 9.1.5 the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller; or
 - 9.1.6 the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- 9.2 If the personal data in question is special category personal data (also known as “sensitive personal data”), at least one of the following conditions must be met:
- 9.2.1 the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
 - 9.2.2 the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
 - 9.2.3 the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - 9.2.4 the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
 - 9.2.5 the processing relates to personal data which is manifestly made public by the data subject;
 - 9.2.6 the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
 - 9.2.7 the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
 - 9.2.8 the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
 - 9.2.9 the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
 - 9.2.10 the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

10 Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- 10.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- 10.2 Where consent is given in a document which includes other matters, the section dealing with consent must be kept clearly separate from such other matters.
- 10.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- 10.4 If personal data is to be processed for a different purpose that is incompatible with the purpose or purposes for which that personal data was originally collected that was not disclosed to the data subject when they first provided their consent, consent to the new purpose or purposes may need to be obtained from the data subject.
- 10.5 If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.
- 10.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

11 Specified, Explicit, and Legitimate Purposes

- 11.1 The Group collects and processes the personal data set out in the data register of this Policy. This includes:
 - personal data collected directly from data subjects.
 - personal data obtained from third parties.
- 11.2 The Group only collects, processes, and holds personal data for the specific purposes set out in Part 24 of this Policy (or for other purposes expressly permitted by Data Protection Law).
- 11.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Group uses their personal data. Please refer to Part 15 for more information on keeping data subjects informed.

12 Adequate, Relevant, and Limited Data Processing

- 12.1 The Group will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 17, below.
- 12.2 Employees, agents, contractors, or other parties working on behalf of the Group may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.
- 12.3 Employees, agents, contractors, or other parties working on behalf of the Group may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

13 Accuracy of Data and Keeping Data Up-to-Date

- 13.1 The Group shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 18, below.
- 13.2 The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

14 Data Retention

- 14.1 The Group shall not keep personal data for any longer than is necessary considering the purpose or purposes for which that personal data was originally collected, held, and processed.
- 14.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- 14.3 For full details of the Group's approach to data retention, including retention periods for specific personal data types held by the Group, please refer to our Data Register (CR08) and Data Retention Procedure (CP07).

15 Secure Processing

- 15.1 The Group shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 31 to 33 of this Policy.
- 15.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
- 15.3 Data security must be always maintained by protecting the confidentiality, integrity, and availability of all personal data as follows:
- only those with a genuine need to access and use personal data, and who are authorised to do so, may access and use it;
 - personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
 - authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

16 Data Protection Impact Assessments and Privacy by Design

- 16.1 In accordance with the Privacy by Design principles, the Group shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.
- 16.2 The principles of Privacy by Design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
- the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
 - the state of the art of all relevant technical and organisational measures to be taken;

- the cost of implementing such measures; and
- the risks posed to data subjects and to the Group, including their likelihood and severity.

16.3 Data Protection Impact Assessments shall be overseen by the Group Company Secretary and shall address the following:

- the type(s) of personal data that will be collected, held, and processed;
- the purpose(s) for which personal data is to be used;
- the Group's objectives;
- how personal data is to be used;
- the parties (internal and/or external) who are to be consulted;
- the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- risks posed to data subjects;
- risks posed both within and to the Group; and
- proposed measures to minimise and handle identified risks.

17 Keeping Data Subjects Informed

17.1 The Group shall provide the information set out in Part 18.2 to every data subject:

- where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

17.2 The following information shall be provided in the form of a privacy notice:

- details of the Group including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection contact;
- the purpose(s) for which the personal data is being collected and will be processed and the lawful basis justifying that collection and processing;
- where applicable, the legitimate interests upon which the Group is justifying its collection and processing of the personal data;
- where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- where the personal data is to be transferred to one or more third parties, details of those parties;

- where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
- details of applicable data retention periods;
- details of the data subject's rights under the UK GDPR;
- details of the data subject's right to withdraw their consent to the Group's processing of their personal data at any time;
- details of the data subject's right to complain to the Information Commissioner's Office;
- where the personal data is not obtained directly from the data subject, details about the source of that personal data;
- where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

18 Data Subject Access

- 18.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Group holds about them, what it is doing with that personal data, and why.
- 18.2 Employees wishing to make a SAR should do using a Subject Access Request Form (CF02), sending the form to the Group Company Secretary at companysecretary@chrysalisgroupservices.co.uk.
- 18.3 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- 18.4 All SARs received shall be handled by the Group Company Secretary and in accordance with the Group's Data Subject Access Request Procedure (CP06).
- 18.5 The Group does not charge a fee for the handling of normal SARs. The Group reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

19 Rectification of Personal Data

- 19.1 Data subjects have the right to require the Group to rectify any of their personal data that is inaccurate or incomplete. They can do so using the Combined Data Change Request Form (CF09).
- 19.2 The Group shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Group of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- 19.3 If any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

20 Erasure of Personal Data

20.1 Data subjects have the right to request that the Group erases the personal data it holds about them in the following circumstances:

- it is no longer necessary for the Group to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- the data subject wishes to withdraw their consent to the Group holding and processing their personal data;
- the data subject objects to the Group holding and processing their personal data (and there is no overriding legitimate interest to allow the Group to continue doing so) (see Part 21 of this Policy for further details concerning the right to object);
- the personal data has been processed unlawfully;
- the personal data needs to be erased in order for the Group to comply with a particular legal obligation.

20.2 Data subjects can request erasure by using the Right to Erasure Request Form (CF10).

20.3 Unless the Group has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

20.4 If any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

21 Restriction of Personal Data Processing

21.1 Data subjects may request that the Group ceases processing the personal data it holds about them. If a data subject makes such a request, the Group shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

21.2 If any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

22 Objections to Personal Data Processing

22.1 Data subjects have the right to object to the Group processing their personal data based on legitimate interests, for direct marketing (including profiling).

22.2 Where a data subject objects to the Group processing their personal data based on its legitimate interests, the Group shall cease such processing immediately, unless it can be demonstrated that the Group's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

22.3 Where a data subject objects to the Group processing their personal data for direct marketing purposes, the Group shall cease such processing promptly.

23 Data Security - Transferring Personal Data and Communications

The Group shall ensure that the following measures are taken with respect to all

communications and other transfers involving personal data:

- 23.1 All emails containing personal data must be encrypted. Microsoft uses TLS (Transport Layer Security) to encryption a connection between computers and between Exchange servers (this is what controls email accounts) and to other servers. TLS doesn't encrypt the message just the connection. If the recipient organisation does not support TLS then the message isn't necessarily encrypted, all Microsoft exchange servers are TLS compliant.
- 23.2 All emails containing personal data must be marked "confidential";
- 23.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;
- 23.4 Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
- 23.5 Personal data contained in the body of an email, whether sent or received, should be copied from the body of the email and stored securely. The email itself should be deleted from the main folder and the deleted folder.
- 23.6 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using a secure delivery service agreed with the recipient.
- 23.7 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential";

24 Data Security - Storage

The Group shall ensure that the following measures are taken with respect to the storage of personal data:

- 24.1 All electronic copies of personal data should be stored securely using passwords and data encryption; The files are stored in OneDrive or SharePoint which has a AES256-CBC encryption (Advanced Encryption Standard with 256-bit key length in Cipher Block Changing mode). If files are stored on a computers HDD/SSD then the computer will have BitLocker turned on. This provides a similar encryption (AES128-CBC by default)
- 24.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- 24.3 All personal data stored electronically is stored on the Cloud (OneDrive, SharePoint, and Exchange emails) with data is backed up 3 times a day with the encryption AES256.
- 24.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Group or otherwise .
- 24.5 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Group and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Group where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to the Group that all suitable technical and organisational measures have been taken);
- 24.6 Access to personal data must be through a password controlled device

25 Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and

disposed of. For further information on the deletion and disposal of personal data, please refer to the Group's Data Register.

26 Data Security - Cease of Trade

- 26.1 Should any member of the Group stop trading due to being purchased by another organisation all data will be transferred over to that service.
- 26.2 If any member of the Group stops trading all together the parent company will be responsible for storing only legally required information electronically and ensuring the remainder is destroyed. All records will continue to be stored in line with statutory guidelines and best practice.
- 26.3 The Group recognises the legal obligation held relating to how long data should be retained for, ICO registration and that data protection laws continue to apply.

27 Data Security - Use of Personal Data

The Group shall ensure that the following measures are taken with respect to the use of personal data:

- 27.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Group requires access to any personal data that they do not already have access to, such access should be formally requested from the relevant Director or the Group Company Secretary.
- 27.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Group or not, without the authorisation of the relevant Director or the Group Company Secretary.
- 27.3 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;
- 27.4 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- 27.5 Where personal data held by the Group is used for marketing purposes, it shall be the responsibility of the Marketing Co-ordinator to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS;

28 Disclosure of Data

- 28.1 The Group will ensure any data held is protected from unauthorised access by using appropriate security methods in relation to the access and storage of the data.
- 28.2 Personal data will not be disclosed to data processors unless a contract/confidentiality agreement is in place defining authorised data usage.
- 28.3 Employees at The Group will not disclose any personal data via the telephone unless the requesters' identity can be formally verified.

29 Use of Third Parties to Manage/ Disclosing Data to Third Parties

- 29.1 The Group will always carry out robust risk assessments and due diligence checks when using a third party to manage or process data. All information security requirements will be detailed in a contract between The Group and the third party.
- 29.2 The Group will not disclose personal data to a third party unless their identity can be formally verified and one of the following conditions are met:

- The Group have given consent to the sharing of the information with the third party
- The data subject or individual holding Lasting Power of Attorney for the data subject have given consent to share the information with the third party or for the third party to request the information
- Sharing the data is essential for lawful purpose for which the data is being processed
- Disclosure is subject to the terms of a formal Information Sharing Protocol
- Disclosure is required by law (including the prevention or detection of crime, apprehension or prosecution of offenders and the assessment or collection of any tax or duty)

- 29.3 The Group will only share sensitive information with a third party if the data subject has given their consent for disclosure or for the third party to request the information, or if disclosure is deemed a best interest decision made in line with the Mental Capacity Act.
- 29.4 Sensitive information will also be disclosed to a third party if the Group is required to share the information by Law or if the disclosure is in the vital interest of the data subject.
- 29.5 In the above circumstances authorisation must be sought from the DPO before disclosure can take place.
- 29.6 Any information shared with third parties will be the minimal amount required to satisfy contractual or legitimate requirements.
- 29.7 Consent in relation to sensitive data must be explicit to the purpose and the decision to disclose should be recorded on the appropriate IT system.

30 Secondary Uses of Data

On occasion The Group may wish to use data for purposes not directly related to the care of the service user e.g. research or audit purposes, commissioning, performance or capacity management.

In such cases, pseudonyms will be used to protect anonymity and maintain confidentiality.

31 Security of Information

- 31.1 The Group has systems in place to manage risk and identify needs in relation to the security of information throughout the organisation.
- 31.2 Risk management is necessary to ensure data is protected and regulatory requirements are met.
- 31.3 The Group will undertake the following actions to ensure information is handled and stored securely:
- 31.3.1. The implementation of a clear desk policy within our office space so that no personal or sensitive information is left unattended and accessible to those unauthorised to view the information
 - 31.3.2. Group IT devices and emails are encrypted
 - 31.3.3. All information asset and processing facilities are protected securely from unauthorised access
 - 31.3.4. Unsupported systems (i.e. software, hardware or applications) are easily identified so they can be removed, replaced or risk assessed
 - 31.3.5. Confidentiality and integrity of information is a priority and will be maintained
 - 31.3.6. The Group's requirements, as identified by information owners, for the availability of information assets and information processing facilities required for operational activities are met
 - 31.3.7. All legal and statutory obligations are met

31.3.8. Security of information will be maintained as per The Group's business continuity plan

31.4 Users will only have access to The Group's systems, data and network if they have formally agreed to comply with this policy.

31.5 This will form part of all employee and contractor contracts and will also be part of mandatory training requirements.

31.6 Unauthorised and illegal use of information assets and information processing facilities is prohibited.

31.7 Use of non-company approved web applications to process confidential information is not permitted without this being approved for use by the Group CEO or CFO.

32 Data Security - IT Security

The Group shall ensure that the following measures are taken with respect to IT and information security:

32.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols.

32.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Group, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method.

32.3 IT staff do not have access to passwords a temporary password will be provided which will mean the employee will log on line to change their password. At that point their password become secure. If they lose the password a request can be made to their line manager to reset enabling them to log on and change their password again.

32.4 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. All employees shall be responsible for installing all security-related updates for existing approved software. A scheduled maintenance service is provided to check devices quarterly

32.5 No software may be installed on any Group-owned computer or device without the prior approval of the relevant Group Director.

33 Organisational Measures

The Group shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

33.1 All employees, agents, contractors, or other parties working on behalf of the Group shall be made fully aware of both their individual responsibilities and the Group's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;

33.2 Only employees, agents, contractors, or other parties working on behalf of the Group that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Group;

33.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;

33.4 All employees, agents, contractors, or other parties working on behalf of the Group

handling personal data will be appropriately trained to do so;

- 33.5 All employees, agents, contractors, or other parties working on behalf of the Group handling personal data will be appropriately supervised;
- 33.6 All employees, agents, contractors, or other parties working on behalf of the Group handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 33.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- 33.8 All personal data held by the Group shall be reviewed periodically, as set out in the Group's Data Retention Policy;
- 33.9 The performance of those employees, agents, contractors, or other parties working on behalf of the Group handling personal data shall be regularly evaluated and reviewed;
- 33.10 All employees, agents, contractors, or other parties working on behalf of the Group handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
- 33.11 All agents, contractors, or other parties working on behalf of the Group handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Group arising out of this Policy and Data Protection Law;
- 33.12 Where any agent, contractor or other party working on behalf of the Group handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Group against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;

34 Record Keeping

- 34.1 The Group will ensure that all service user care records are accessible to all authorised employees who require access to such records in order to perform their duties.
- 34.2 All service user care records should be:
 - Clear concise and free from technical terminology or jargon
 - Free from abbreviation
 - Factually accurate and relevant
 - Free from personal opinion or irrelevant information
 - Clearly marked with the date and time if the record is pertaining to care provided or a service user incident
 - Any paper records should be legible and written in indelible, black ink
 - Alterations to paper records should be scored out with a single line. Correction fluid may not be used if an error is made
- 34.3 The Group's service user records will be documented and stored securely, electronically. Paper records will only be used in the event of a system failure and these will be scanned and updated onto the system once the fault is rectified, then disposed of securely.
- 34.4 All service user care records will be documented in a consistent, professional manner and will adhere to Health Care Record Keeping Standards.
- 34.5 Any service user safeguarding records regarding children will be kept until the child reaches the age of 25 (age of maturity plus 7 years) unless there is reason to keep the record for a longer period.

35 Freedom of Information

- 35.1 The Group is only required to provide information under the Freedom of Information Act 2000 in respect of the activities that it carries out whilst under contract with a public authority. As such, The Group is not required to respond to FOI requests received directly from members of the public in relation to any other of its commercial activities. If such a request is received, the Registered Manager should refer the requesting party to the scope of the legislation and politely decline to provide the information.
- 35.2 Upon receipt of an FOI request, the Registered Manager will endeavour to ensure that the requested information is collated and returned to the contracting public authority to allow them to meet the 20-working day deadline of the legislation. Prior to sending any information it should be checked for any personal data, which should be redacted prior to sending.
- 35.3 In certain circumstances The Group may be asked for our views as to whether certain information should be released before the public body decides as to how to respond. The person responsible for making this decision for The Group would be the Registered Manager.
- 35.4 If The Group provides any information to a public body on the understanding that it is confidential, this should be highlighted on the documents provided. If information has not been provided to a public body on a confidential basis, the public body may consult with The Group as to whether any exemptions under the legislation may apply (for example prejudicing commercial interests).

36 Accountability and Record-Keeping

- 36.1 The Group Company Secretary is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines. The contents of this policy will be reviewed on annual basis, sooner should changes in the law or legislation dictate.
- 36.2 The Group shall always follow a privacy by design approach when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing presents a significant risk to the rights and freedoms of data subjects (please refer to Part 17 for further information).
- 36.3 All employees, agents, contractors, or other parties working on behalf of the Group shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Group policies.
- 36.4 The Group's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.
- 36.5 The Group shall keep written internal records of all personal data collection, holding, and processing on a data register, which shall incorporate the following information:
- the name and details of the Group, its Group Company Secretary, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
 - the purposes for which the Group collects, holds, and processes personal data;
 - the Group's legal basis or bases (including, but not limited to, consent, the mechanism(s) for obtaining such consent, and records of such consent) for collecting, holding, and processing personal data;
 - details of the categories of personal data collected, held, and processed by the Group, and the categories of data subject to which that personal data relates;

- details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;
- details of how long personal data will be retained by the Group;
- details of personal data storage, including location(s);
- detailed descriptions of all technical and organisational measures taken by the Group to ensure the security of personal data.

37 Transferring Personal Data to a Country Outside the UK

37.1 The Group may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

37.2 Personal data may only be transferred to a country outside the UK if one of the following applies:

- The UK has issued adequacy regulations confirming that the personal data will receive an adequate level of protection (referred to as 'adequacy decisions', 'adequacy regulations', or 'partial findings of adequacy'). Such regulations may apply to a country as a whole, organisation(s), framework(s) or mechanism(s), or to data covered by specific legislation. Since 1 January 2021, transfers of personal data from the UK to EEA countries have continued to be permitted. Pre-existing EU Commission adequacy decisions in effect as at 31 December 2020 are also recognised, subject to ongoing review by the UK Government.
- Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct, or an approved certification mechanism. Standard contractual clauses include the International Data Transfer Agreement issued by the Information Commissioner's Office and the International Data Transfer Addendum to the current EU Commission Standard Contractual Clauses (set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021), issued by the Information Commissioner's Office. (Contracts entered into on the basis of the old EU Commission Standard Contractual Clauses prior to 21 September 2022 will continue to provide appropriate safeguards until 21 March 2024.)

37.3 The transfer is made with the informed and explicit consent of the relevant data subject(s).

37.4 The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Group; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Group's legitimate interests.

38 Data Breach Notification

38.1 All personal data breaches must be reported immediately to the Group Company Secretary. A Data Breach form must also be completed CF01.

38.2 If an employee, agent, contractor, or other party working on behalf of the Group becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. All evidence relating to the personal data breach in question should be carefully retained.

- 38.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Group Company Secretary must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 38.4 If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Group Company Secretary must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 38.5 Data breach notifications shall include the following information:
- The categories and approximate number of data subjects concerned;
 - The categories and approximate number of personal data records concerned;
 - The name and contact details of the Group Company Secretary (or other contact point where more information can be obtained);
 - The likely consequences of the breach;
 - Details of the measures taken, or proposed to be taken, by the Group to address the breach including, where appropriate, measures to mitigate its possible adverse effects.
- 38.6 The Data Breach process is detailed in (CP05)

Related Documents

CP01	Data Protection Impact Assessment Procedure
CP04	Data Protection Audit Guidance Notes
CP05	Data Breach Procedure
CP06	Data Subject Access Request Procedure
CP07	Data Retention and Disposal Procedure
CP08	Data Breach Guidance Notes
CP09	Data Retention Guidance Notes
CP10	Data Breach Register
CF01	Data Breach Form
CF02	Data Subject Access Request Form
CF03	Data Protection Impact Assessment Questionnaire
CF04	Data Protection Audit Checklist Form
CF09	Combined Data Change Request
CF10	Right to Erasure Request Form
CF17	Data Protection Impact Assessment Form
CR08	Data Register
CM23	Confidentiality & Access to Information Policy