



DATA SECURITY AND PROTECTION POLICY

Version 4	June 2022
Agreed by SMT	June 2022
Review date	June 2024

1. Introduction	3
2. Scope.....	3
3. Policy Framework.....	3
4. Responsibilities	3
5. Definitions and Abbreviations	6
6. The Data Protection Principles.....	8
7. The Rights of Data Subjects	8
8. Lawful, Fair, and Transparent Data Processing.....	9
9. Consent	10
10. Specified, Explicit, and Legitimate Purposes	11
11. Adequate, Relevant, and Limited Data Processing.....	11
12. Accuracy of Data and Keeping Data Up to Date	12
13. Data Retention.....	12
14. Secure Processing	12
15. Record-Keeping	12
16. Privacy by Design and DPIAs.....	13
17. Keeping Data Subjects Informed	14
18. Data Subject Access	15
19. Rectification of Personal Data	16
20. Erasure of Personal Data	16
21. Restriction of Personal Data Processing.....	17
22. Data Portability.....	17
23. Objections to Personal Data Processing.....	18
24. Automated Processing, Decision-Making, and Profiling	18
25. Direct Marketing.....	19
26. Data Security - Transferring Personal Data and Communications	20
27. Data Security - Storage	20
28. Data Security - Disposal	21
29. Data Security	21
30. Organisational Measures.....	22
31. Transferring Personal Data Outside the UK.....	23
32. Data Breach Notification	24
33. Implementation and Review	24
34. Approval	24
35. Change History	25
Appendix A - Documents supporting the Data Security & Protection Framework	27

1. Introduction

- 1.1 This is a Policy of Age UK East London, a Private Limited Company by guarantee without share capital use of 'Limited' exemption registered in England under number 07687015, whose registered office is at 2nd Floor 82 Russia Lane, Bethnal Green, London, England, E2 9LU ("the Company").
- 1.2 It sets out the Company's obligations regarding Data Security and Protection and the rights of board members, employees, volunteers, donors, clients, service users, business contacts and suppliers ("Data Subjects") in respect of their Personal Data under Data Protection Law.
- 1.3 This Policy sets out the Company's approach to the collection, processing, transfer, storage, and disposal of Personal Data.

2. Scope

- 2.1 The Company is committed not only to the letter, but also to the spirit of the law and places great 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.
- 2.2 All Policies and Procedures set out or referred to in this document and related policies and procedures in the Framework must be followed at all times by the Company, its Board Members, employees, agents, contractors, volunteers and other parties ("Parties") acting or working on its behalf in all locations, including when working from home.
- 2.3 The Company recognises that flexible working arrangements, in particular home working, are important in providing a better work-life balance and ensuring the health and safety of Parties acting or working on its behalf. Whilst working from home, it is equally important to protect Personal Data and the rights and privacy of individuals as set out in this Policy.

3. Policy Framework

- 3.1 The Company's **Data Security and Protection Policy** is a fundamental and essential part of the Company's **Data Security and Protection Framework**, which in turn is part of its overall policy framework.
- 3.2 As the Company's primary policy in this subject area, this Policy should be consulted first on matters relating to data security and protection.
- 3.3 The Framework and this Policy are defined and supported by many other policies, procedures, forms, notices and register a schedule. A schedule of these documents is to be found in Appendix A to this Policy.

4. Responsibilities

- 4.1 The Company's **Chief Executive Officer** is ultimately responsible to the Board of Trustees for all data security and protection matters relating to the Company.
- 4.2 As part of their governance role, the **Trustees and Board Members** monitor the Company's strategic objectives and assist in directing how it is managed, including in relation to data security and protection.

- 4.3 Except where more specifically indicated, the Company's **Information Governance Lead** is responsible for the administration of this policy.
- 4.4 The Company's **Operations and Human Resources Manager** is responsible for ensuring that all Parties acting or working on behalf of the Company are given appropriate briefing and training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.
- 4.5 **Board Members, senior managers, managers and supervisors** are responsible for ensuring that all Parties acting or working on behalf of the Company comply with this and related policies and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance. Where possible and appropriate, such measures, and, in particular training, should be made available remotely to home workers.
- 4.6 The Company's **Data Protection Officer (DPO)** is Nicholas Birch of Exigia Ltd, whose registered office is at Kemp House, 152-160 City Road, London EC1V 2NX, whose business address is at 62A Robson Road, Worthing, West Sussex BN12 4EF and whose email address is dpo@exigia.com. The DPO is responsible for:
- a) Reviewing this and related policies, procedures, forms and registers regularly to ensure that they comply with current Data Protection Law and best practice.
 - b) Reviewing the Company's data protection compliance by means of Data Protection Audits.
 - c) Providing advice and guidance to the Company on Data Protection legislation and the content and interpretation of this policy. The Data Protection Officer should always be consulted in the following circumstances:
 - i) if there is any uncertainty relating to the lawful basis on which Personal Data is to be collected, held, and/or Processed;
 - ii) if consent is being relied upon in order to collect, hold, and/or Process Personal Data;
 - iii) if there is any uncertainty relating to the retention period for any particular type(s) of Personal Data;
 - iv) if any new or amended privacy notices or similar privacy-related documentation are required;
 - v) 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);
 - vi) if a Personal Data Breach (suspected or actual) has occurred;
 - vii) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect Personal Data;
 - viii) if there are any questions relating to the implementation and maintenance of security measures in a home working environment;

- ix) if Personal Data is to be shared with third parties (whether such third parties are acting as Controllers or Processors);
- x) 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;
- xi) when any significant new Processing activity is to be carried out, or significant changes are to be made to existing Processing activities, which could require a Data Protection Impact Assessment;
- xii) when Personal Data is to be used for purposes different to those for which it was originally collected;
- xiii) if any automated Processing, including profiling or automated decision-making, is to be carried out; or
- xiv) if any assistance is required in complying with the law applicable to direct marketing.

5. Definitions and Abbreviations

BYOD	means devices or the use of devices that belong to Parties other than the Company to connect to the Company's IT and communications systems or perform IT or communications functions in place of devices belonging to the Company;
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;
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 Company is the Controller of all Personal Data relating to staff, business contacts, clients, suppliers, donors and volunteers used in our business for our commercial purposes except where it Processes Personal Data on behalf of another Controller, thereby acting as a Processor;
Data Subject Access Request	means the right granted to Data Subjects under the General Data Protection Regulation (GDPR) to access any Personal Data an organisation holds on them. This is known as a Data Subject Access request (SAR);
Data Protection Law	All legislation and regulations in force from time to time regulating the use of Personal Data and the privacy of electronic communications including, but not limited to, the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the "UK GDPR"), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of Section 3 of the European Union (Withdrawal) Act 2018, the Data Protection Act 2018, The Privacy and Electronic Communications Regulations 2003 as amended, and any successor legislation.
Data Subject	means a living, identified, or identifiable natural person about whom the Company holds Personal Data;
Framework	means the Company's Data Security & Protection framework of policies, procedures, processes and practices;
IT Systems	means the IT and communications devices, infrastructure, computing environment, data and any and all other relevant equipment belonging to the Company and any such items leased, lent, borrowed or otherwise used by the Company;

Parties (acting or working on behalf of the Company)	except where otherwise stated means Board Members, employees, agents, contractors, volunteers and other parties (“Parties”) acting on or working on its behalf;
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;
Processor	means a natural or legal person or organisation which Processes Personal Data on behalf of a Controller. For the purposes of this Policy, the Company is the Processor of any Personal Data that it Processes on behalf of another Controller;
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;

6. The Data Protection Principles

6.1 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. Controllers are responsible for, and must be able to demonstrate, such compliance. All Personal Data must be:

- a) Processed lawfully, fairly, and in a transparent manner in relation to the Data Subject;
- b) 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;
- 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. 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;
- e) 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;
- f) 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.

7. The Rights of Data Subjects

7.1 The GDPR sets out the following key rights applicable to Data Subjects:

- a) The right to be informed;
- b) the right of access;
- c) the right to rectification;
- d) the right to erasure (also known as the 'right to be forgotten');
- e) the right to restrict Processing;
- f) the right to data portability;
- g) the right to object; and
- h) rights with respect to automated decision-making and profiling.

8. Lawful, Fair, and Transparent Data Processing

8.1 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 GDPR states that Processing of Personal Data shall be lawful if at least one of the following applies:

- a) the Data Subject has given consent to the Processing of their Personal Data for one or more specific purposes;
- b) 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;
- c) the Processing is necessary for compliance with a legal obligation to which the Controller is subject;
- d) the Processing is necessary to protect the vital interests of the Data Subject or of another natural person;
- e) 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 Controller; or
- f) the Processing is necessary for the purposes of the legitimate interests pursued by the 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.

8.2 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:

- a) 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);
- b) the Processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment, social security, and social protection law (insofar as it is authorised by law);
- c) 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;
- d) the 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;

- e) the Processing relates to Personal Data which is manifestly made public by the Data Subject;
- f) the Processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- g) 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;
- h) 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 further conditions and safeguards set out in Data Protection Law;
- i) 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
- j) the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes with a basis in 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.

9. Consent

9.1 If Consent is relied upon as the lawful basis for collecting, holding, and/or Processing Personal Data, the following shall apply:

- a) 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.
- b) 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.
- c) 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.
- d) 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.

- e) If Special Category Personal Data is PProcessed, 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.
- f) 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.

9.2 Where appropriate, the Company's Data Consent Form will be used to record the Data Subject's agreement and/or withdrawal of Consent.

10. Specified, Explicit, and Legitimate Purposes

- 10.1 The Company collects and Processes the Personal Data set out in its **Data Processing Register**. This includes:
 - a) Personal Data collected directly from Data Subjects and
 - b) Personal Data obtained from third parties.
- 10.2 The Company only collects, Processes, and holds Personal Data for the specific purposes set out in its Data Processing Register (or for other purposes expressly permitted by Data Protection Law).
- 10.3 Data Subjects must be kept informed at all times of the purpose or purposes for which the Company uses their Personal Data. Refer to the relevant section of this Policy for more information on keeping Data Subjects informed.

11. Adequate, Relevant, and Limited Data Processing

- 11.1 The Company 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) and as contained in its Data Processing Register.
- 11.2 Parties acting or working on behalf of the Company 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.
- 11.3 Parties acting or working on behalf of the Company 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.

12. Accuracy of Data and Keeping Data Up to Date

- 12.1 The Company 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.
- 12.2 The accuracy of Personal Data shall be checked when it is collected and at 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.

13. Data Retention

- 13.1 The Company shall not keep Personal Data for any longer than is necessary in light of the purpose or purposes for which that Personal Data was originally collected, held, and Processed.
- 13.2 When Personal Data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- 13.3 Full details of the Company's approach to data retention, including retention periods for specific Personal Data types held by the Company, are contained in its **Data Retention & Disposal Policy**.

14. Secure Processing

- 14.1 The Company 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 this Policy.
- 14.2 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.
- 14.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all Personal Data as follows:
- a) only those with a genuine need to access and use Personal Data and who are authorised to do so may access and use it;
 - b) Personal Data must be accurate and suitable for the purpose or purposes for which it is collected, held, and Processed; and
 - c) authorised users must always be able to access the Personal Data as required for the authorised purpose or purposes.

15. Record-Keeping

- 15.1 The Company shall keep written internal records including a **Data Processing Register** of all Personal Data collection, holding, and Processing, which shall incorporate the following information:
- a) details of the categories of Personal Data collected, held, and Processed by the Company, and the categories of Data Subject to which that Personal Data relates;

- b) the purposes for which the Company collects, holds, and Processes Personal Data;
- c) the Company'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;
- d) details of Personal Data storage, including location(s);
- e) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of Personal Data.
- f) the name and details of any Company or applicable third-party data transfers (including Processors, Sub-Processors and other Controllers with whom Personal Data is shared);
- g) details of any transfers of Personal Data outside the UK including all mechanisms and security safeguards;
- h) details of how long Personal Data will be retained by the Company (please refer to the Company's Data Retention & Disposal Policy);

16. Privacy by Design and DPIAs

- 16.1 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:
- a) the nature, scope, context, and purpose or purposes of the collection, holding, and Processing;
 - b) the state of the art of all relevant technical and organisational measures to be taken;
 - c) the cost of implementing such measures; and
 - d) the risks posed to Data Subjects and to the Company, including their likelihood and severity.
- 16.2 In accordance with the privacy by design principles:
- a) The Company shall carry out Data Protection Impact Assessment (DPIA) Threshold Assessments for all new programmes, projects, procedures or products ('Programmes') in order to:
 - i) ensure that data protection, security and privacy issues have been properly considered
 - ii) determine whether completing a full DPIA is required
 - iii) decide whether to complete a DPIA as good privacy by design practice
 - b) The Company shall carry out DPIAs for any and all new Programmes 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.
 - c) The Company's Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:

- i) the type(s) of Personal Data that will be collected, held, and Processed;
 - ii) the purpose(s) for which Personal Data is to be used;
 - iii) the Company's objectives;
 - iv) how Personal Data is to be used;
 - v) the parties (internal and/or external) who are to be consulted;
 - vi) the necessity and proportionality of the data Processing with respect to the purpose(s) for which it is being Processed;
 - vii) risks posed to Data Subjects;
 - viii) risks posed both within and to the Company; and
 - ix) proposed measures to minimise and handle identified risks.
- 16.3 Details of both DPIA Threshold Assessments and DPIAs are contained in the Company's DPIA Procedures document.

17. Keeping Data Subjects Informed

- 17.1 The Company shall provide the information set out in the next section to every Data Subject:
- a) where Personal Data is collected directly from Data Subjects, those Data Subjects will be informed of its purpose at the time of collection; and
 - b) where Personal Data is obtained from a third party, the relevant Data Subjects will be informed of its purpose:
 - i) if the Personal Data is used to communicate with the Data Subject, when the first communication is made; or
 - ii) if the Personal Data is to be transferred to another party, before that transfer is made; or
 - iii) 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:
- a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its Data Protection Officer;
 - b) the purpose(s) for which the Personal Data is being collected and will be Processed and the lawful basis justifying that collection and Processing;
 - c) where applicable, the legitimate interests upon which the Company is justifying its collection and Processing of the Personal Data;
 - d) where the Personal Data is not obtained directly from the Data Subject, the categories of Personal Data collected and Processed;
 - e) where the Personal Data is to be transferred to one or more third parties, details of those parties;

- f) 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 the relevant section of this Policy for further details);
- g) details of applicable data retention periods;
- h) details of Data Subjects' rights under Data Protection Law;
- i) details of Data Subjects' right to withdraw their consent to the Company's Processing of their Personal Data at any time;
- j) details of Data Subjects' right to complain to the Information Commissioner's Office (the "supervisory authority" under Data Protection Law);
- k) where the Personal Data is not obtained directly from the Data Subject, details about the source of that Personal Data;
- l) 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
- m) 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 Under The Data Protection Legislation, Data Subjects are entitled to make Subject Access Requests (SARs) at any time to find out about the Personal Data which the Company holds about them, what it is doing with that Personal Data, and why.
- 18.2 As the Company collects, holds, and processes Personal Data about Staff, volunteers, business contacts, donors and service users, the Company is a Controller for the purposes of the Data Protection Legislation.
- 18.3 When acting as a Controller, the Company and its Staff must follow its **Data Subject Access Procedure** when responding to SARs related to the Personal Data it controls.
- 18.4 As the Company also processes Personal Data on behalf of other organisations, it is also a Processor for the purposes of the Data Protection Legislation.
- 18.5 When acting as a Processor, the Company must inform its Controller whenever it receives a SAR relating to the Personal Data that they control and follow the Controller's SAR Process rather than the Company's Processes.
- 18.6 The Company's handling of SARs of all types shall be supervised by the Company's Data Protection Officer and will be conducted by the Company's management in accordance with the Company's **Data Subject Access Procedures**.
- 18.7 All Parties acting or working on behalf of the Company, including those working from home, must ensure that all Personal Data that they are working

with is kept organised and, wherever possible, only stored and Processed within the Company's system(s) in order to enable rapid search and retrieval

- 18.8 All Parties acting or working on behalf of the Company must cooperate fully with the Company's management and Data Protection Officer in handling any SAR received.

19. Rectification of Personal Data

- 19.1 Data Subjects have the right to require the Company to rectify any of their Personal Data that is inaccurate or incomplete.
- 19.2 The Company shall rectify the Personal Data in question, and inform the Data Subject of that rectification, within one month of the Data Subject informing the Company 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 In the event that 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.
- 19.4 All Parties acting or working from home on behalf of the Company must ensure that all the Personal Data that they work with is kept organised and, wherever possible, only Processed within and using the Company's systems in order to enable rapid and/or centralised rectification. They must also cooperate with the Company in ensuring that any Personal Data held by them at their homes that requires rectification is rectified within the relevant time limits.

20. Erasure of Personal Data

- 20.1 Data Subjects have the right to request that the Company erases the Personal Data it holds about them in the following circumstances:
- a) it is no longer necessary for the Company to hold that Personal Data with respect to the purpose(s) for which it was originally collected or Processed;
 - b) the Data Subject wishes to withdraw their consent to the Company holding and Processing their Personal Data;
 - c) the Data Subject objects to the Company holding and Processing their Personal Data (and there is no overriding legitimate interest to allow the Company to continue doing so)
 - d) the Personal Data has been Processed unlawfully;
 - e) the Personal Data needs to be erased in order for the Company to comply with a particular legal obligation or;
 - f) the Personal Data is being held and Processed for the purpose of providing information society services to a child.
- 20.2 Unless the Company 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.

20.3 In the event that 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).

20.4 All Parties acting or working from home on behalf of the Company must ensure that all the Personal Data that they work with is kept organised and, wherever possible, only Processed within and using the Company's systems in order to enable rapid and/or centralised erasure. They must also co-operate with the Company in ensuring that any Personal Data held by them at their homes that requires erasure is erased within the relevant time limits.

21. Restriction of Personal Data Processing

21.1 Data Subjects may request that the Company ceases Processing the Personal Data it holds about them. If a Data Subject makes such a request, the Company 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 In the event that 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).

21.3 All Parties acting or working from home on behalf of the Company must ensure that all the Personal Data that they work with is kept organised and, wherever possible, only Processed within and using the Company's systems in order to enable rapid and/or centralised application of restrictions. They must also co-operate with the Company in ensuring that any Personal Data held by them at their homes that requires the application of restrictions is restricted within the relevant time limits.

22. Data Portability

22.1 The Company Processes Personal Data using automated means.

22.2 Where Data Subjects have given their consent to the Company to Process their Personal Data in such a manner, or the Processing is otherwise required for the performance of a contract between the Company and the Data Subject, Data Subjects have the right, under Data Protection Law, to receive a copy of their Personal Data and to use it for other purposes (namely transmitting it to other Controllers).

22.3 To facilitate the right of data portability, the Company shall make available all applicable Personal Data to Data Subjects in the following formats:

- a) Hard copy
- b) Personal Data format files (.pdf)
- c) Microsoft Word files (.doc and .docx)

d) Microsoft Excel files (.xls and .xlsx)

22.4 Where technically feasible, if requested by a Data Subject, Personal Data shall be sent directly to the required Controller.

22.5 All requests for copies of Personal Data shall be complied with within one month of the Data Subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the Data Subject shall be informed.

23. Objections to Personal Data Processing

23.1 Data Subjects have the right to object to the Company Processing their Personal Data based on legitimate interests, for direct marketing (including profiling), and Processing for scientific and/or historical research and statistics purposes.

23.2 Where a Data Subject objects to the Company Processing their Personal Data based on its legitimate interests, the Company shall cease such Processing immediately, unless it can be demonstrated that the Company'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.

23.3 Where a Data Subject objects to the Company Processing their Personal Data for direct marketing purposes, the Company shall cease such Processing promptly.

23.4 Where a Data Subject objects to the Company Processing their Personal Data for scientific and/or historical research and statistics purposes, the Data Subject must, under Data Protection Law, "demonstrate grounds relating to his or her particular situation". The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

24. Automated Processing, Decision-Making, and Profiling

24.1 The Company uses Personal Data in automated decision-making Processes as follows:

a) No purposes

24.2 The Company uses Personal Data for profiling purposes as follows:

a) No purposes

24.3 The activities described in this section are generally prohibited under Data Protection Law where the resulting decisions have a legal or similarly significant effect on Data Subjects unless one of the following applies:

a) the Data Subject has given their explicit consent;

b) the Processing is authorised by law; or

c) the Processing is necessary for the entry into, or performance of, a contract between the Company and the Data Subject.

- 24.4 If Special Category Personal Data is to be Processed in this manner, such Processing can only be carried out if one of the following applies:
- a) the Data Subject has given their explicit consent; or
 - b) the Processing is necessary for reasons of substantial public interest.
- 24.5 Where decisions are to be based solely on automated Processing (including profiling), Data Subjects have the right to object, to challenge such decisions, request human intervention, to express their own point of view, and to obtain an explanation of the decision from the Company. Data Subjects must be explicitly informed of this right at the first point of contact.
- 24.6 In addition to the above, clear information must be provided to Data Subjects explaining the logic involved in the decision-making or profiling, and the significance and envisaged consequences of the decision or decisions.
- 24.7 When Personal Data is used for any form of automated Processing, automated decision-making, or profiling, the following shall apply:
- a) appropriate mathematical or statistical procedures shall be used;
 - b) technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
 - c) all Personal Data to be Processed in this manner shall be secured in order to prevent discriminatory effects arising.

25. Direct Marketing

- 25.1 The Company is subject to certain rules and regulations when marketing its products and/or services.
- 25.2 The prior consent of Data Subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls subject to the following limited exception:
- a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer in question has been given the opportunity to opt-out of marketing when their details were first collected and in every subsequent communication from the Company.
- 25.3 The right to object to direct marketing shall be explicitly offered to Data Subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.
- 25.4 If a Data Subject objects to direct marketing, their request must be complied with promptly. A limited amount of Personal Data may be retained in such circumstances to the extent required to ensure that the Data Subject's marketing preferences continue to be complied with.

26. Data Security - Transferring Personal Data and Communications

- 26.1 The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving Personal Data:
- a) All emails containing Personal Data must be encrypted;
 - b) All Parties acting or working from home on behalf of the Company must, whenever possible, access and Process Personal Data when connected to the Company's Virtual Private Network ("VPN").
 - c) All emails containing Personal Data must be marked "confidential";
 - d) Personal Data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances. All Parties acting or working on behalf of the Company working from home must ensure that their home network is secure at all times and that, where applicable and reasonably possible, any and all security software or firmware updates for network equipment such as modems and routers are installed. Advice and assistance is available from the Company.
 - e) Personal Data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
 - f) Personal Data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
 - g) Where Personal Data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
 - h) Where Personal Data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using registered post or an approved courier service and must be signed for on receipt. Personal Data must not be transferred to home workers in hardcopy form except in exceptional circumstances.
 - i) 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".

27. Data Security - Storage

- 27.1 The Company shall ensure that the following measures are taken with respect to the storage of Personal Data:
- a) All electronic copies of Personal Data should be stored securely using secure passwords and encryption where practical.
 - b) 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 and the Company will provide suitable storage

equipment to Parties acting or working on behalf of the Company working from home who are likely to be Processing Personal Data.

- c) All Personal Data stored electronically should be backed up regularly with backups stored onsite and offsite. Backups should be encrypted where practical.
- d) The storage of Personal Data on mobile devices (including, but not limited to, laptops, tablets, and smartphones), whether such devices belong to the Company or otherwise should be limited to the extent absolutely necessary for the performance of relevant work. Furthermore, Parties acting or working on behalf of the Company working from home must comply with all security and other instructions and limitations imposed by the Company.
- e) Personal Data may only be transferred to, stored on, accessed from or Processed on devices belonging to Parties acting or working on behalf of the Company to the extent absolutely necessary for the performance of the relevant work, and only where the work in question is being undertaken by a home worker. In the case of (BYOD) devices belonging to Parties acting or working on behalf of the Company, Personal Data may only be transferred to, stored on, accessed from, or Processed on such devices where the party in question has agreed to comply fully with the letter and spirit of this Policy and Data Protection Law and the Company's **Bringing Your Own Devices to Work Policy** (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken).

28. Data Security - Disposal

- 28.1 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.
- 28.2 For further information on the deletion and disposal of Personal Data, please refer to the Company's **Data Retention & Disposal Policy**.

29. Data Security

- 29.1 The Company intends to achieve high standards of Data Security and Protection, particularly in relation to the Processing of Personal Data.
- 29.2 All Parties acting or working on behalf of the Company shall abide by the provisions of the Company's **IT Security Policy** at all times.
- 29.3 The Company aims to demonstrate its attainment of high standards in data security and protection through compliance with relevant benchmarks and by achieving certification where possible. In particular it demonstrates its standards through, but not limited to:
 - a) The NHS **Data Security and Protection Toolkit**
 - b) The National Cyber Security Centre's **Cyber Essentials** scheme
- 29.4 The Company shall ensure that the following measures are taken with respect to the use of Personal Data:

- a) No Personal Data may be shared informally and if any Party acting or working on behalf of the Company requires access to any Personal Data that they do not already have access to, such access should be formally requested from the Caldicott Guardian;
- b) No Personal Data may be transferred to any employee, agent, contractor, or other Party, whether such Parties are acting or working on behalf of the Company or not, without the authorisation of the Caldicott Guardian;
- c) Personal Data must be handled with care at all times and should not be left unattended or on view to unauthorised Parties or others at any time;
- d) 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;
- e) All Parties acting or working on behalf of the Company working from home must ensure that they use all reasonable efforts to comply with the provisions of this section and the Company's **IT Security Policy** including, for example, setting aside a specific room or part of their home (ideally behind a lockable door, in a room with lockable windows) for home working, particularly when handling Personal Data.
- f) The Company recognises that home workers may not always be able to ensure a degree of security comparable to the Company's premises, but all reasonably practicable efforts should be made to ensure the adequate security at all times;
- g) Where Personal Data held by the Company is used for marketing purposes, it shall be the responsibility of the Caldicott Guardian 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.

30. Organisational Measures

- 30.1 The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of Personal Data:
- a) All Parties acting or working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be given access to a copy of this Policy;
 - b) Only Parties acting or working on behalf of the Company 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 Company;
 - c) 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;
 - d) All Parties acting or working on behalf of the Company handling Personal Data will be appropriately trained to do so;
 - e) All Parties acting or working on behalf of the Company handling Personal Data, including those working from home, will be supervised by appropriate methods;

- f) All Parties acting or working on behalf of the Company 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;
- g) Methods of collecting, holding, and Processing Personal Data shall be regularly evaluated and reviewed;
- h) All Personal Data held by the Company shall be reviewed periodically, as set out in the Company's **Data Retention & Disposal Policy**;
- i) The performance of Parties acting or working on behalf of the Company handling Personal Data shall be regularly evaluated and reviewed;
- j) All Parties acting or working on behalf of the Company handling Personal Data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
- k) All Parties acting or working on behalf of the Company handling Personal Data must ensure that any and all of their employees or agents who are involved in the Processing of Personal Data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;
- l) Where any Party acting or working on behalf of the Company handling Personal Data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

31. Transferring Personal Data Outside the UK

- 31.1 The Company does not currently store or transfer any Personal Data outside the UK.
- 31.2 If the Company were to transfer ('transfer' includes making available remotely) Personal Data to countries outside of the UK it would take into account that the UK GDPR restricts such transfers in order to ensure that the level of protection given to Data Subjects is not compromised.
- 31.3 The transfer of Personal Data to a country outside of the UK would take place only if one or more of the following applies:
 - a) The UK has issued regulations confirming that the country in question ensures an adequate level of protection (referred to as 'adequacy decisions' or 'adequacy regulations'). From 1 January 2021, transfers of Personal Data from the UK to EEA countries will continue to be permitted. Transitional provisions are also in place to recognise pre-existing EU adequacy decisions in the UK.
 - b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK (this includes those adopted by the European Commission prior to 1 January 2021), an approved code of conduct, or an approved certification mechanism.
 - c) The transfer is made with the informed and explicit consent of the relevant Data Subject(s).

- d) 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 Company; 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 Company's legitimate interests.

32. Data Breach Notification

32.1 All Personal Data Breaches must be reported immediately under the terms of the Company's **Security Incident and Data Breach Policy** and by following the Company's **Security Incident and Data Breach Procedure**.

32.2 This provision includes handling Personal Data Breaches relating to Personal Data being Processed by Parties acting or working from home on behalf of the Company using either personal computers or devices or those provided by the Company.

33. Implementation and Review

33.1 This Policy shall be deemed effective as of 27th June 2022. Nothing in this document shall have retroactive effect and shall thus apply only to matters occurring on or after this date.


33.2 This document will be updated as necessary to reflect current best practice, official guidance, and in line with current legislation.

33.3 This document will be reviewed regularly and normally at least every two years.

33.4 The latest version of this document will be made readily available to all relevant parties.

34. Approval

This document has been approved and authorised by:

Name:	Geetha Umaasuthan
Position:	Director of Finance and Operations
Date:	27/6/2022
Due for Review by:	26/06/2024
Signature:	

35. Change History

Version	Section	Issue	Change	Approval	Date
4.0	All	Review	Mostly minor. Appendix A versions updated.	DPO	24/06/2022
3.0	All	New Data Security and Protection Framework	Many detailed changes plus a reorganisation of the policy framework and documents subordinate or supporting this policy.		
3.1	Multiple and 5	Repetition	References to multiple staff groups etc., replaced with the defined term "Parties".		
	4.1 - 4.5 31.1	Responsibilities needed expansion	References to the responsibilities the CEO and Trustees added, the latter since its inclusion in the DS&P Toolkit. Reference to training and briefing widened.		
	Appendix A	Document structure	The schedule of supporting documents moved to a new Appendix A.		
3.2	Throughout	Scope	Altered the phrase "... working on behalf ...") to "acting or working on behalf ...".		

Version	Section	Issue	Change	Approval	Date
	5	Definitions	Section renamed as Definitions and Abbreviations and extra entries added		
	25	Incorrect paragraph structure	25.3 reduced to an a) bullet under Section 25.2. Subsequent section numbers adjusted downwards.		
	27.1 e)	BYOD	Added reference to the new Bringing your Own Devices to Work Policy		
	29 / 30	Overlap	Sections merged and subsequent section numbers adjusted (downwards).		
	Appendix A	Document versions	Documents added and version numbers updated.		

Appendix A - Documents supporting the Data Security & Protection Framework

The following list may not be exhaustive, and the document version numbers (where included) are current only on the effective date of this Policy.

Document	Type	Version	Notes
Bringing Your Own Device to Work Policy	Policy	1.0	
Confidentiality Policy	Policy	-	
Cookies Notice	Notice	-	
Data Processing Register	Register	-	
Data Retention & Disposal Policy	Policy	4.0	
Data Security and Protection Policy	Policy	4.0	This policy
Data Security and Protection Training Policy	Policy	4.0	
Data Subject Access Procedures	Procedures	4.0	
Data Subject Access Request Form	Form	4.0	
Data Subject Consent Form	Form	4.0	
DPIA Procedures	Procedures	4.0	
IT Security Policy	Policy	4.0	
National Data Opt-out Assessment	Policy	-	DSPT 1.2.4
Notice to Staff - Use of Public W-Fi	Notice	1.1	
Privacy Notice	Notice	-	Website etc.
Processing by External Suppliers Policy, incorporating Questionnaire and Monitoring Plans	Policy	4.0	
Records Management and Data Handling Policy	Policy	4.0	
Security Incident and Data Breach Policy	Policy	4.0	
Security Incident and Data Breach Procedure	Procedure	4.0	
Training Needs Assessment			