Data Protection

1. **Purpose:**
   1.1. The purpose of this document is to state the Data Protection policy of Ormiston Families.

2. **Persons Affected:**
   2.1. The Data Protection policy and procedure is applicable to Ormiston Families Trustees, employees, volunteers, partners, voluntary groups and third parties and agents who Ormiston have authorised access.

3. **Policy:**
   3.1. In order to operate efficiently, Ormiston Families has to collect and use information about the people with whom it works. These may include members of the public, service users, current, past and prospective employees, clients, customers, contractors, suppliers and partner organisations.
   3.2. Personal information must be handled and dealt with properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.
   3.3. Ormiston Families regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between Ormiston Families and those with whom it carries out business. Ormiston Families will ensure that it treats personal information correctly in accordance with the law.
   3.4. Ormiston Families fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998 (DPA).
   3.5. This policy applies to all personal information created or held by Ormiston Families, in whatever format. This includes but is not limited to paper, electronic and email.
   3.6. The DPA does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act (FOIA) 2000, but should also be considered fairly and lawfully.

4. **Definitions:**
   4.1. **Caldicott Guardian**: A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.
   4.2. **Consent:** Any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed. Consent can be withdrawn after it has been given. Where data is 'sensitive', express consent must be given for processing this data.
   4.3. **Data Controller:** Person, company or organisation who determines the purpose and manner of the processing of personal data, in other words, the body responsible for the data (for example, Ormiston Families).
   4.4. **Data Subject:** Any living individual who is the subject of personal data.

4.5. **Data Subject Access Request:** The right of an individual to inspect all personal data relating to him or her held by a data controller. The data controller must produce the requested information in an intelligible and, unless this is impracticable, permanent format.

4.6. **Encryption:** Is a means of preventing anyone other than those who have a key from accessing data, be it in an email, on a PC or on a storage device.

4.7. **Mobile devices:** Where we refer to 'mobile devices', the definition is intended to be broad and includes memory sticks, mobile phones, tablets, PDAs, netbooks and laptops.

4.8. **Personal data:** Information relating to a named or otherwise identifiable individual. This includes any expressions of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

4.9. **Processing (data):** Covers almost anything, which is done with or to the data, including:

4.9.1. obtaining data,

4.9.2. recording or entering data onto the files,

4.9.3. holding data, or keeping it on file without doing anything to it or with it,

4.9.4. organising, altering or adapting data in any way,

4.9.5. retrieving, consulting or otherwise using the data,

4.9.6. disclosing data either by giving it out, by sending it on email, or simply by making it available,

4.9.7. combining data with other information,

4.9.8. erasing or destroying data.

4.10. Sensitive personal data: Personal data containing information relating to the racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life or criminal history of a data subject.

5. Responsibilities:

5.1. The DPA stipulates that anyone processing personal data must comply with 8 principles of good practice. These principles are legally enforceable.

5.2. The principles require that personal information:

5.2.1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;

5.2.2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;

5.2.3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;

5.2.4. Shall be accurate and where necessary, kept up to date;

5.2.5. Shall not be kept for longer than is necessary for that purpose or those purposes;

5.2.6. Shall be processed in accordance with the rights of data subjects under the Act;

5.2.7. Shall be kept secure i.e. protected by an appropriate degree of security;

5.2.8. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protect.

5.3. The DPA provides conditions for the processing of any personal data. It also makes a distinction between personal data and "sensitive" personal data (see section 4.10 above). Sensitive personal data requires stricter conditions of processing.

5.4. Ormiston Families is a data controller under the Data Protection Act 1998. The Resources Director is accountable for ensuring compliance with this policy. The day-to-day responsibilities are delegated to Service and/or Programme Managers.

5.5. Directors are responsible for ensuring that Programme Areas they have responsibility for have processes and procedures in place that comply with the DPA and this policy. They are responsible for ensuring that data is appropriately protected or that controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged.

5.6. Ormiston Families will appoint 'Caldicott Guardians' to provide advice to ensure that where health related personal information is shared (particularly in relation to patients, children and vulnerable adults) it is done properly, legally and ethically.

5.7. All employees who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal and/or sensitive information is kept and processed in accordance with the DPA and this policy.

5.7.1. In particular, staff must not attempt to access personal data that they are not authorised to view.

5.7.2. Failure to comply with the DPA may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/prosecution.

5.8. If a contractor, partner organisation or agent of the Ormiston Families is appointed or engaged to collect, hold, process or deal with personal data on behalf of Ormiston Families, or if they will do so as part of the services they provide to Ormiston Families, the lead manager must ensure that personal data is kept in accordance with the principles of the DPA and this policy.

5.8.1. Security and Data Protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with Ormiston Families.

6. Procedures:

6.1. Ormiston Families promotes **information sharing** where it is in the best interests of the subject. A data exchange agreement must be in place prior to any work commencing.

6.1.1. Ormiston Families has information sharing protocols in place and will comply with the standards established in those protocols.

6.1.2. Where appropriate, Ormiston Families' Caldicott Guardians will provide advice.

6.2. When information is shared with other organisations or partners, a formal information sharing agreement must be in place that is signed by all parties.

6.2.1. Responsibility for its implementation lies with the Service Manager responsible.

6.3. An individual may **request a copy of any data** held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request (SAR) under the DPA.

6.3.1. Ormiston Families will provide information on how to make a SAR on Ormiston Families' website.

6.3.2. The statutory £10 fee is payable for all access to records applications.

6.4. Ormiston Families employees may **share information** when it is in the best interests of the data subject and when failure to share data may carry risks to vulnerable groups and individuals.

6.5. Personal data must not be disclosed about a third party, except in accordance with the DPA.

6.6. If employees believe it is necessary to disclose information about a third party to a person requesting data, you must seek advice from the Programme Area Manager or Service Director, whoever is the most senior.

6.6.1. All contractors and individuals working for or on behalf of Ormiston Families must ensure identity checks are undertaken before providing personal data over the telephone.

6.6.2. Information must always be shared in a secure and appropriate manner and in accordance with the information type and classification.

6.6.3. Ormiston Families will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

6.7. If an individual **requests that personal data held about them be updated** because it is wrong, incomplete or inaccurate, the position should be investigated thoroughly, with reference to the source of information.

6.7.1. A caution should be marked on the person's file to indicate uncertainty regarding accuracy until the investigation is complete.

6.7.2. Ormiston Families will work with the person to either correct the data and/or allay their concerns.

6.7.3. An individual is entitled to apply to the court for a correcting order which would authorise Ormiston Families to rectify, block, erase or destroy the inaccurate information as appropriate.

6.8. Individuals can **request Ormiston Families to stop processing data**. If data is properly held for marketing purposes for example, an individual is entitled to require that this is discontinued as soon as possible.

6.8.1. Requests must be made in writing, but generally all written or oral requests should be heeded as soon as they are made. The individual must be informed in writing that the processing has been discontinued ("cessation").

6.8.2. If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have

given their consent, if the data is held in connection with a contract with the person, if Ormiston Families is fulfilling a legal requirement, or, if the person's vital interests are being protected.

6.8.3. Valid written requests must be responded to in writing within 21 calendar days upon receipt.

6.9. **Complaints** about how Ormiston Families processes data under the DPA and responses to subject access requests are dealt with by the Operations Director.

6.9.1. Complaints are to be put in writing and sent to the Operations Director.

6.10. The Information Commissioner maintains a **public register of data controllers**, in which Ormiston Families is registered.

6.10.1. The DPA requires every data controller processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

6.10.2. The Operations Director will review and update the Data Protection Register annually prior to notification to the Information Commissioner.

6.11. Ormiston Families will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation.

6.11.1. Any breach of this policy should be investigated in accordance with the mandatory procedures specified in the Information Security Incident Management Policy and Procedure.

6.11.2. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct.

7. Document Approval: Duncan Turner, Resources Director.

8. Revision History: January 2017.