

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 Families 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.

3.3.1. 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 General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) and other relevant legislation protecting privacy rights.

3.4.1. 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.

3.4.2. The GDPR and the DPA regulation 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. **Consent:** Any freely given specific, informed and unambiguous indication of the data subject's wishes by which he or she 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 Consent can be withdrawn after it has been given.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.

4.2. Data Controller: An organisation which determines the purposes for which personal data is processed and is legally accountable for the personal data that it collects and uses or contracts with others to process on its behalf.

4.3. Data Processor: In relation to personal data, any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

4.4. Data Subject: Any living individual who is the subject of personal data.

4.5. 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. combining data with other information,
- 4.9.2. disclosing data either by giving it out, by sending it on email, or simply by making it available,
- 4.9.3. erasing or destroying data,
- 4.9.4. holding data, or keeping it on file without doing anything to it or with it,
- 4.9.5. obtaining data,
- 4.9.6. organising, altering or adapting data in any way,
- 4.9.7. recording or entering data onto the files,
- 4.9.8. retrieving, consulting or otherwise using the data.

4.10. Special category data: Personal data containing information relating to the racial or ethnic origin, political opinions, religious beliefs, trade union membership, processing of genetic and biometric data, physical or mental health, or sexual life.

5. Responsibilities:

5.1. Ormiston Families will apply the following data protection principles and all the other requirements of data protection to the management of all personal data through the information life cycle.

- 5.2.** The principles require that personal information shall be:
- 5.2.1. accurate and where necessary, kept up to date (“accuracy”);
 - 5.2.2. adequate, relevant and limited to what is necessary for those purposes (“data minimisation”)
 - 5.2.3. collected or created for specific explicit and lawful purposes and not be further processed in a manner that is incompatible with those purposes (“purpose limitation”);
 - 5.2.4. kept safe from unauthorised access, processing, accidental or deliberate loss or destruction (“integrity and confidentiality”);
 - 5.2.5. processed fairly and lawfully and in a way that is transparent to the data subject (“Lawfulness, fairness and transparency”);
 - 5.2.6. retained in a form that can identify individuals for no longer than is necessary for that purpose (“storage limitation”).
- 5.3.** Under data protection law, Ormiston Families must also:
- 5.3.1. allow personal data to be transferred to other countries only if it maintains the same level of protection for the privacy rights of the data subjects concerned.
 - 5.3.2. meet its legal obligations as a data controller or processor, including data protection by design and default, data protection impact assessment, maintaining records of processing activities, measures to ensure the security of processing and handling of data breaches.
 - 5.3.3. proactively inform data subjects about its data processing activities and their rights under the law.
- 5.4.** The GDPR and DPA provides conditions for the processing of any personal data. It also makes a distinction between personal data and special category personal data (see glossary for definitions). Special category data requires stricter conditions of processing.
- 5.5.** Ormiston Families is a data controller and where applicable a data processor under the GDPR and Data Protection Act 2018.
- 5.5.1. The Privacy Officer is accountable for ensuring compliance with this policy.
 - 5.5.2. The day-to-day responsibilities are delegated to Service and/or Programme Managers.
- 5.6.** 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.
- 5.7.** All employees who hold or collect personal data are responsible for their own compliance with the data protection policy and associated data protection legislation and must ensure that personal and/or special category information is kept and processed in accordance with 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 data protection policy 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 GDPR and Data Protection Act 2018 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.

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. An information sharing agreement must be in place *prior* to any work commencing.

- 6.2.2. Responsibility for the implementation of an information sharing agreement 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 GDPR and DPA.

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

- 6.3.2. Ormiston Families must provide all such information in a readable form within 1 month of the request

- 6.3.3. Ormiston Families should provide such information free of charge unless the request is excessive or manifestly unfounded.

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 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.
- 6.6.4. We will publish this information on our website and where appropriate in printed formats.
- 6.6.5. We will review the content of these privacy notices regularly and inform our data subjects of any significant changes which may affect them.
- 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 and responses to subject access requests are dealt with by the Privacy Officer.

6.9.1. Complaints are to be put in writing and sent to the Privacy Officer.

6.10. The Information Commissioner's Office (ICO) maintains a **public register of data controllers**, in which Ormiston Families is registered (reference Z4976802).

6.10.1. The ICO 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 Privacy Officer 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.

6.11.2. Where the data breach is likely to result in a risk to the rights and freedoms of data subjects, the Privacy Officer will liaise with the Information Commissioners Office and report the breach in line with regulatory requirements within 72 hours of discovery.

6.11.3. The Privacy Officer will also recommend, where necessary, actions to inform data subjects and reduce risks to their privacy arising from the breach.

7. Document Approval: Allan Myatt, Chief Executive.

8. Revision History: July 2018