DATA PROTECTION

1.	**SUMMARY**	The data protection policy explains how Ormiston Families complies with the principles of data protection, and acts as a statement of intent to which the organisation, employees or third parties must abide.			
2.	**RESPONSIBLE PERSON**	Head of Quality and Governance			
3.	**ACCOUNTABLE DIRECTOR**	Income Generation & Marketing Director			
4.	**APPLIES TO:**	This policy is applicable to all Ormiston Families trustees, employees (permanent and temporary), partners, volunteers and third parties and agents who have access to the personal data Ormiston Families process.			
5.	**GROUPS / INDIVIDUALS WHO HAVE OVERSEEN THE DEVELOPMENT OF THIS POLICY:**	Tracy Pez, Data Protection Consultant, Data Protection People. Kate Higgs, Income Generation & Marketing Director / Privacy Officer Justin Claxton, Head of Quality and Governance / Deputy Privacy Officer Mark Proctor, Caldicott Guardian / Operations Director. Duncan Turner, Senior Information Risk Officer / Finance Director and Company Secretary.			
6.	**GROUPS WHICH WERE CONSULTED AND HAVE GIVEN APPROVAL:**	Senior Leadership Team (SLT)			
7.	**EQUALITY IMPACT ANALYSIS COMPLETED:**	**Policy Screened**	-	**Template Completed**	-
8.	**RATIFYING COMMITTEE(S) & DATE OF FINAL APPROVAL:**	21/09/23, Board of Trustees, 08/03/24.			
9:	**VERSION:**	2.1			
10:	**AVAILABLE ON:**	**Hive**	Sept. 23	**Website**	Sept. 23
11.	**RELATED DOCUMENTS**	Information Sharing and Confidentiality policy Records Management policy Personal Data Breach procedure IT Security policy DPIA Screening Tool			
12.	**DISSEMINATED TO:**	All staff			
13.	**DATE OF IMPLEMENTATION:**	September 2023			
14.	**DATE OF NEXT FORMAL REVIEW:**	September 2024			

DOCUMENT CONTROL

Date	Version	Action	Amendments
May 2018	1.0	Policy updated and implemented	N/A
February 2023	1.1	Policy amended	Clarification and edits.
August 2023	2.0	Policy reviewed and redrafted by external consultant.	Substantial amendments made to refine roles and responsibilities and align with information governance framework.
October 2023	2.1	Policy amended	Minor edits to ensure consistent reference to related policies and procedures.

Contents

1. Introduction

1.1 The data protection policy explains how Ormiston Families complies with the principles of data protection and acts as a statement of intent to which the organisation, employees or third parties must abide.

2. Policy Statement

2.1 Organisations processing personal data in the UK are required to comply with the UK data protection legislation framework, namely the Retained General Data Protection Regulation (EU) 2016/679 (UK GDPR) and the Data Protection Act 2018 (DPA).

2.2 The UK GDPR sets out that everyone has the fundamental right to the protection of personal data concerning him or her. It states that the protection of natural persons should be technology neutral and should not depend on the techniques used. All employees, contractors and service users of Ormiston Families services have a right to expect that they can trust us to use their data fairly and lawfully.

2.3 It is the policy of Ormiston Families to comply with all relevant data protection legislation, including the UK GDPR and the DPA and any subsequent amendments.

Ormiston Families will:

- ensure that we comply with the Data Protection Principles (as set out in legislation) and the Caldicott Principles.
- meet our legal obligations as laid down by the UK GDPR, DPA, Health and Social Care Act 2015, Access to Health Records Act 2000, and any other relevant legislation.
- respect the rights of all data subjects.

2.4 The Data Protection Principles are:

- Accountability – Ormiston Families must acknowledge and understand our role and responsibilities whether we are acting as a data controller or data processor. We ensure this by having appropriate governance of how data is used, at the appropriate level of oversight at management level.
- Lawfulness, Fairness, and Transparency – Ormiston Families will ensure that we have a lawful basis for all processing carried out, process data fairly and in a way which would be expected, and we must be transparent informing individuals how and why we process their data.
- Purpose Limitation – Ormiston Families will ensure that we only use data for the original reason for which it was collected and not for other incompatible purposes.
- Data Minimisation – Ormiston Families will ensure we process only the minimum personal data for the agreed purposes.
- Accuracy - Ormiston Families will ensure that the data we process is accurate and up to date.
- Storage Limitation - Ormiston Families will ensure that the personal data we process is only kept for the minimum time necessary and then securely deleted in line with our

own policies and other relevant regulations or legislation. We have a retention schedule which must be adhered to.

2.5 The Caldicott Principles are specifically focussed on the use of confidential healthcare data. These principles shall be considered when considering clinical data.

The principles are:

- justify the purpose(s) for using confidential information - Ormiston Families will ensure that use of personal confidential data is clearly defined, scrutinised, documented, and reviewed by an appropriate guardian.
- don't use personal confidential data unless it is absolutely necessary - Ormiston Families will ensure that personal confidential data items should not be included in any processing unless it is essential. The need for customers and service users to be identified should be considered at each stage.
- use the minimum necessary personal confidential data - Ormiston Families will ensure that where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is used as is necessary for a given function to be carried out.
- access to personal confidential data should be on a strict need-to-know basis - Ormiston Families will ensure that only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see.
- everyone with access to personal confidential data should be aware of their responsibilities - Ormiston Families will ensure that all personnel handling personal confidential data should be fully aware of their responsibilities and obligations to respect patient confidentiality
- comply with the law - Ormiston Families will ensure that our use of personal confidential information is always lawful. We have a Privacy Officer and Caldicott Guardian responsible for ensuring that the organisation complies with these principles and legal requirements.
- the duty to share information can be as important as the duty to protect patient confidentiality - Ormiston Families must ensure that we share information when it is in the best interests of individuals and lawful to do so.

2.6 Under data protection legislation, Ormiston Families must also:

- allow personal data to be transferred to other countries only if there are appropriate transfer mechanisms and safeguards in place.
- meet our 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.
- proactively inform data subjects about our data processing activities and their rights under the law.

2.7 Ormiston Families are registered as a data controller with the Information Commissioner's Office (ICO). We are registered as 'Ormiston Families (registration number Z4976802)

and 'Ormiston Families Enterprises Limited' (registration number ZA068805). These registrations are updated annually.

3. Scope of this 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 (and their families), current, past and prospective employees, clients, customers, contractors, suppliers and partner organisations.

3.2 Personal data is defined as any data that (alone or with other information) can be used to identify a living individual and its processing is regulated by the DPA and the UK GDPR. Anonymised or aggregated data is not personal data. For clarity, individuals can be identified by various means including their name and address, telephone number or email address. Reference numbers are also personal data.

3.3 Ormiston Families regards the lawful and correct treatment of personal information as critical to its successful operations and all 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 or processed by any other means.

3.4 Some personal information is more sensitive and is referred to as special category data under data protection legislation. This includes any data relating to health, race or ethnic origin, genetic data, information about an individual's sexual orientation and any criminal data.

3.5 Whilst all personal data should be treated confidentially, special category data must be treated with an enhanced level of diligence.

3.6 The UK GDPR and DPA provide conditions for the processing of any personal data. Special category data requires stricter conditions of processing.

3.7 Whilst the UK GDPR and DPA apply only to living individuals, The Common Law Duty of Confidentiality also applies to the data Ormiston Families process and this exceeds an individual's death. This means data regarding a deceased person must still be treated appropriately and confidentially.

4. Who this policy applies to

4.1 This policy is applicable to all Ormiston Families trustees, employees (permanent and temporary), volunteers, partners, volunteers and third parties and agents who have access to the personal data Ormiston Families process.

4.2 This policy applies to all personal data for which Ormiston Families process either as the data processor or data controller.

5. Roles and responsibilities

5.1 Ormiston Families is often a data controller but, in some circumstances, we are a data processor under the UK GDPR and DPA. It is the responsibility of all staff, whether permanent or temporary, and all contractors to:

- observe this policy and all associated procedures.
- collect and process personal data and special category personal data in accordance with data protection legislation and this policy and associated procedures.
- report any actual or suspected personal data breaches in accordance with our Personal Data Breach procedure.
- understand that breaches of this policy may lead to disciplinary action, up to and including dismissal.

The following roles have specific responsibilities for data protection within our organisation. These are in addition to other responsibilities held and detailed within our Data Protection and Information Governance policies and other related documents.

Ormiston Families have a Privacy Officer and a Caldicott Guardian who are responsible for ensuring all personal data is processed in line with legislation and in a fair and transparent manner.

5.2 The Privacy Officer is:

- responsible for monitoring and ensuring compliance with this policy and overseeing Ormiston Families data processing activities.
- able to provide advice and is the first point of contact in the organisation for data protection matters.
- responsible for co-operating with and acting as the contact point for the ICO (UK's supervisory authority).
- the contact point for data subjects regarding all issues related to the processing of his or her data.
- responsible for escalating any serious concerns to the Board.

The Privacy Officer is the Income Generation & Marketing Director, Kate Higgs.

The Deputy Privacy Officer is the Head of Quality and Governance, Justin Claxton.

5.3 The Caldicott Guardian is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly and in compliance with this policy and associated procedures. The Caldicott Guardian operates in accordance with the 8 Caldicott principles to ensure people's information is kept confidential and used appropriately (see s. 2.5 above).

The Caldicott Guardian is the Operations Director, Mark Proctor.

5.4 The Senior Information Risk Owner (SIRO) is responsible for managing information security risk and implementing measures to prevent them.

The SIRO is the Finance Director and Company Secretary, Duncan Turner.

5.5. The Caldicott Guardian and the SIRO are jointly responsible for working together to ensure that data is processed confidentially and compliantly.

5.6 There will be a Data Champion from each business area and service that will help channel information on data protection within their department, and ensure tasks are completed as requested by the Privacy Officer.

The Data Champion will undergo regular training and will be the 'go-to' person responsible for overseeing data privacy matters in their business area.

The Data Champions are responsible for encouraging a privacy culture in their business areas and service, ensuring any concerns or queries, especially regarding potential data breach issues, are expediently escalated to the organisation's Privacy Officer.

5.7 Directors are responsible for ensuring that the services they have responsibility for have processes and procedures in place that comply with the UK GDPR, DPA and this policy. Directors have overall responsibility for ensuring that data is appropriately protected and where necessary controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged.

5.8 Business, Service and/or Operations Managers are responsible for the day-to-day oversight of data processing activities across the organisation and within their respective business areas and services.

5.9 All Ormiston Families employees who process personal data for any purpose are responsible for their own compliance with this and other data protection related policies and associated data protection legislation. All employees must ensure that personal and/or special category information is kept and processed in accordance with Ormiston Families policies.

5.10 All Ormiston Families employees will receive appropriate training and management and will:

- ensure information is destroyed when it has reached the end of its retention period and is no longer required.
- ensure they record all data appropriately and maintain complete, accurate, and up to date records, saving information in designated and secure locations.
- immediately upon receipt of an individual rights request by (or on behalf of) an individual related to information held about them, or any other data subject, immediately notify their line manager and appropriately log the access request.
- not attempt to access personal data that they are not authorised to view.
- not send any personal information to unauthorised recipients, or outside of the United Kingdom without the authority of the Privacy Officer.
- observe all forms of guidance, codes of practice and procedures related to the collection and use of personal information.
- process appropriate information, and only in accordance with the purposes for which it is to be used by Ormiston Families to meet its service needs or legal requirements.
- understand fully the purposes for which Ormiston Families uses personal information.

6. Personal Data Breach incidents

6.1 Ormiston Families will always treat any data breach as a serious issue.

Any data breach, suspected or actual, must be reported to the Privacy Officer without delay and in accordance with the *Personal Data Breach* procedure. The Privacy Officer will assess the severity of a breach and determine the measures to take.

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

6.3 The Privacy Officer will lead on ensuring mitigating actions to contain the breach, reduce the risks to individuals and prevent recurrence are taken.

The Privacy Officer will also recommend, where necessary, actions to inform data subjects.

6.4 If the data breach is considered a 'serious incident', staff will consult and follow Section 5 of the *Serious Incident* policy in addition to the procedural requirements of this policy.

A serious incident is an adverse event, whether actual or alleged, which results in or risks significant:

- harm to Ormiston Families' beneficiaries, staff, volunteers or any others who come into contact with our organisation through its work,
- loss of Ormiston Families' money or assets,
- damage to Ormiston Families' property, and/or
- harm to Ormiston Families' work or reputation.

7 Data Sharing with Third Parties

7.1 Ormiston Families promotes information sharing where it is in the best interests of the data subject and it is lawful to do so.

7.2 When information is shared within the organisation and with other organisations and partners it will be done so in accordance with the *Information Sharing and Confidentiality* policy.

7.3 When information is shared with other organisations or partners, data security and data protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with Ormiston Families. A separate Data Sharing Agreement or a Data Processing Agreement may also be required and advice should be sought from the Privacy Officer where necessary. A Data Protection Impact Assessment (DPIA) may also be required. In such cases, the *DPIA Screening Tool* will be used to assess if a full DPIA is required.

A contract or relevant data sharing agreement must be in place prior to any work commencing. This is without exception.

Responsibility for the implementation of an information sharing agreement lies with the Service Manager responsible. The lead manager must ensure that personal data is processed in accordance with the principles of the UK GDPR and DPA and this policy.

8 Requests from Individuals

8.1 Individuals have certain rights which apply in some circumstances over their data. These rights are:

- the right of access,
- the right of rectification,
- the right of erasure,
- the right to restrict processing,
- the right to data portability,
- the right to object,
- Rights regarding automated decision making and profiling.

8.2 It is important all employees are aware that an individual can make a request to exercise one of their rights verbally or in writing at any time using a *Data Subject Access Request* form. All such requests must be forwarded to the Privacy Officer without delay.

Ormiston Families must respond to all requests within 1 month of the request being received.

On occasion a request may come from a third party. Ormiston Families will ensure the recipient is authorised to receive information before any personal data is shared.

8.3 In some circumstances, Ormiston Families employees may be asked to share information about individuals in other circumstances. Ormiston Families will consider each request on its merits and will consider whether the requested information is to be shared in accordance with the *Information Sharing and Confidentiality* policy. Ormiston Families will ensure there is a lawful basis for all sharing.

All employees must seek advice from the Privacy Officer, Operations Manager or Operations Director before disclosing information about an individual to a third party.

Identity checks must always be undertaken before providing personal data over the telephone.

Information must always be shared in a secure and appropriate manner and in accordance with Section 7.20 of the *Information Sharing and Confidentiality* policy.

8.4 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. We will publish this information on our website and where appropriate in printed formats in our privacy notice. Our privacy notice will be updated regularly and we will inform our data subjects of any significant changes which may affect them.

8.5 Ormiston Families employees will create, amend, retain and dispose of staff and service user records in accordance with the *Records Management* policy.

9. Training

9.1 All staff will undertake mandatory online training in UK GDPR (Advanced) and Cyber Security during induction and thereafter as often as deemed necessary by the Privacy Officer.

9.2 Trustees and volunteers will undertake mandatory online training in UK GDPR (Advanced) during induction and thereafter as often as deemed necessary by the Privacy Officer.

9.3 Directors, Operations Managers and/or Service Managers are responsible for ensuring that all staff undertake relevant further training relative to their specific role(s) and responsibilities.

10. Dissemination and implementation

10.1 The Data Protection policy will be disseminated to all managers via email by the Head of Quality and Governance. The Data Protection policy will be disseminated and available to all staff via the intranet's policies page.

11. Monitoring

11.1 Compliance with this policy will be monitored by the Privacy Officer including via quarterly internal audit and support and challenge meetings. Findings shall be reported directly to the SIRO, Caldicott Guardian, and if required to Trustees.

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 as outlined in Section 15 of the *IT Security* policy.

12. Review

12.1 The Data Protection policy will be reviewed annually by the Head of Quality and Governance.