Data Protection Policy

Document Ref:	Version No:	Summary of Changes:	Author:	Release Date:	Approved By:
OR26	3	Full review of policy and split with confidentiality and information sharing	Sarah O'Neil	Feb 2018	QSGC
OR26	4	Appendix A removed	Sarah O'Neil	May 2018	QSGC
OR26	5	Review minor changes to wording	Fey Audin	Feb 2019	QSGC
OR26	6	Added 7. Data Breach information mirrored in Confidentiality policy	Fey Audin	Sept 2019	QSGC
OR26	7	Full Review Added Appendix A Data Breach Response Plan	Fey Audin	Jan 2020	PSC

Contributors: Paul Moran
Renewal date: Jan 2022

Contents

1 Introduction 4

2. General data protection regulation principles 4

3 Information covered by the General Data Protection Regulation 5

4 Scope 6

5 Data protection framework 6

6 Employee responsibilities 6

7 Data Breach 7

8 Associated documents 8

Appendix A: Data Breach Response Plan 9

Fair Ways Vision, Mission and Values

Our vision
To build an institution that makes a difference to society and leaves a legacy greater than ourselves and our contributions.

Our mission
Making a difference through passionate care, support and education.

Our values
Our values form the heart of the work we do, defined by Fair Ways people, for Fair Ways people. These are the values by which we operate, by which we are governed, and to which we are held accountable.

We therefore expect every individual within the organisation to *play their part*:

PROFESSIONAL ATTITUDE	**A**CCEPTING	**R**EFLECTIVE	**T**RANSPARENT
· We do what we say we will · We approach challenges with optimism and enthusiasm · We don't judge, we notice · We put the needs of the service before our own personal gains	· We don't give up on people · We value all individuals and are willing to challenge them · We embrace each other's differences as much as our similarities · We accept responsibility for our actions	· We give feedback, we invite feedback, we listen to feedback · We look inward before we look outward · We learn as much from our mistakes as from our successes · We listen to each other, learn from each other and grow together	· We are always willing to explain why · We have the courage to be open and honest · We earn trust through our transparency · We live by our values even when no-one is watching

1 Introduction

1.1 This policy document sets out the principles and practices adopted by Fair Ways for assuring their compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)

1.2 Fair Ways provides services in education, fostering, training, outreach, health and residential care for children, young people and families. As this policy considers a range of services offered by Fair Ways, all children, young people and adults will be referred to in this policy as 'service users' for ease of reference.

1.3 There is a need to collect personal information about people with whom Fair Ways deals in order to carry out its business and provide its services. Such people include service users, employees and foster carers (present, past and prospective). The information includes name, address, email address, date of birth, private and confidential information and sensitive information. In addition, we may occasionally be required to collect and use certain types of such personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g. on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with the GDPR.

1.4 The lawful and proper treatment of personal information by Fair Ways is extremely important to the success of the services and in order to maintain the confidence of our service users and employees. We ensure that Fair Ways treats personal information lawfully and correctly.

2. General data protection regulation principles

2.1 Personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to

the purposes for which they are processed, are erased or rectified without delay ('accuracy');

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 are processed; ('storage limitation');

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 ('integrity and confidentiality').

3 Information covered by the General Data Protection Regulation

3.1 The GDPR definition of "personal data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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 natural person." Individuals can be identified by various means including their name and address, telephone number and/or Email address.

3.2 Article 9 of the GDPR gives details of special categories of data. These categories are personal data revealing:

- racial or ethnic origin;
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- data concerning health
- sexual life or sexual orientation

3.3 It is prohibited for special category data to be processed unless one of the following applies:

- Explicit consent has been gained
- The data is required by an employer
- It is in the vital interests of the data subject
- The data processing is carried out by a religious or philosophical not for profit body with appropriate safeguards

- The data is being processed for legal claims / defence
- It is in the public interest
- It is required for medical purposes

4 Scope

4.1 All Fair Ways' employees are within the scope of this policy including permanent employees, temporary employees, zero hour employees, foster carers and contractors.

5 Data protection framework

5.1 The Chief Operations Officer has ultimate responsibility for compliance with this policy and the GDPR but has delegated leadership for data protection within Fairways to be fulfilled by the Paul Moran (Director of IT, Marketing & Communications). Specific responsibilities of the data protection lead will include operational responsibility for reviewing policies and procedures, ensuring relevant data protection training is delivered to employees, supporting and advising employees on day-to-day protection matters as they arise and ensuring data compliance audits are carried out.

5.2 The management team is jointly responsible for compliance with this policy, with each manager performing the lead role within their respective area of the business. All senior managers have the responsibility for ensuring that systems and processes within their departments comply with the requirements of the GDPR.

5.3 All persons working for Fair Ways, who have access to Person Identifiable Data, are responsible for ensuring that any personal data which they hold is kept securely and is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party.

6 Employee responsibilities

6.1 All employees will, through appropriate training and responsible management:

- Observe all forms of guidance and procedures about the collection and use of personal information
- Understand fully the purposes for which Fair Ways uses personal information

- Collect and process appropriate information, only in accordance with the purposes for which it is to be used to meet the service needs or legal requirements
- Ensure information is destroyed when it is no longer required in accordance with the provisions of the GDPR and in line with Fair Ways data retention schedule.
- Notify their line manager and the data protection lead on receipt of any request by or on behalf of an individual for information held about them
- Understand that breaches of this policy may result in disciplinary action

7 Data Breach

7.1 All employees have a legal duty of confidence to keep person-identifiable and confidential information private and not to divulge information accidentally. Employees may be held personally liable for a breach of confidence and must not:

- Talk about person-identifiable or confidential information in public places or where they can be overheard.
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents
- Leave a computer terminal unattended, which is logged on to a system where person-identifiable or confidential information can be accessed

7.2 Steps must be taken to ensure physical safety and security of person-identifiable or business confidential information held in paper format and on computers.

7.3 Passwords must be kept secure and must not be disclosed to unauthorised persons. Employees must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. More information about acceptable use of Fair Ways IT systems can be found in the Acceptable Usage Policy (DOC REF OR54).

7.4 Fair Ways take any breach of data seriously. The breach could arise from a theft, a deliberate attack on the system, the unauthorised use of personal data by an employee, accidental loss or equipment failure. However the breach occurs, it will be responded to and managed appropriately. A Data Breach Response Plan (Appendix A) for dealing with any breach is in place which includes a recovery plan, damage limitation, an assessment of the risks associated with the breach, informing the appropriate people and reviewing the response and updating the security of the information.

7.5 Any breach of the Confidentiality Policy, depending on the severity of the breach could result in one of the following sanctions:

- Temporary or permanent withdrawal of ICT hardware, software or services from the offending individual
- Disciplinary action in accordance with Fair Ways disciplinary procedure as detailed in the employee handbook
- Criminal or civil proceedings

8 Associated documents

- Confidentiality policy (DOC REF OR26A)
- Information sharing policy (DOC REF OR26B)
- Acceptable usage policy (DOC REF OR54)
- Mobile phone policy (DOC REF OR10)
- Consent & Individual rights Policy (DOC REF OR26C)

Appendix A: Data Breach Response Plan

Fair Ways will adhere to the General Data Protection Regulation (the GDPR) 2018 and Article 29 Data Protection Working Party - Guidelines on Personal data breach notifications under regulations 2016/679 {adopted 3 October 2017- As last revised and adopted on 6 February 2018}

Data Response Team (DRT)

Data Response Team (DRT) is responsible for breach of data.

Information Governance Lead:	Paul Moran (Director of IT, Marketing & Communications)
Data Response Team Coordinator:	Fey Audin (Data Co-ordinator)
Corporate Data Breach Responders:	Mac McHugh (Chief Executive Officer)
Corporate Data Breach Responders:	Vivien Sheath (Chief Financial Officer)
Communications Data Breach Responder:	Paul Moran (Director of IT, Marketing & Communications)
IT Data Breach Responder:	Sean Kitchin (IT Lead)
Departmental Data Breach Responder:	Relevant Operations Directors

Procedure in the event of a data breach.

The data breach is to be reported by email and phone to the relevant director of the service, the Director of IT (paul.moran@fairways.co) and the data protection coordinator (fey.audin@fairways.co).

The report of the breach of data must include:

a) what has happened;
b) when and how you found out about the breach;
c) the people that have been or may be affected by the breach;
d) what you are doing as a result of the breach; and
e) who we should contact if we need more information and who else you have told.

The Director of IT and Data Protection Coordinator will:

a) Refer to Guidelines on Personal data breach notifications under regulations 2016/679 {adopted 3 October 2017- As last revised and adopted on 6 February 2018}.

b) Carry out a self-assessment online with Information Commissions Office (https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach)

c) Based on a) and b) carry out a plan of action to manage the breach and mitigate its effect.

d) Review the incident and record and follow through any lessons learned.

Where necessary the Data Protection Coordinator will contact the ICO on 03031231113 for guidance and clarification.

Guidelines on Personal data breach notifications under regulations 2016/679 {adopted 3 October 2017- As last revised and adopted on 6 February 2018}
Annexure 7 below

A. Flowchart showing notification requirements