Organisational

Data Protection Policy

Document Ref:	Version No:	Summary of Changes:	Author:	Release Date:	Approved By:	Lessons Learned Ref:
OR26	3	Full review of policy and split with confidentiality and information sharing	Sarah O'Neil	Feb 2018	QSGC	N/A
OR26	4	Appendix A removed	Sarah O'Neil	May 2018	QSGC	N/A
OR26	5	Review minor changes to wording	Fey Audin	Feb 2019	QSGC	N/A
OR26	6	Added 7. Data Breach information mirrored in Confidentiality policy	Fey Audin	Sept 2019	QSGC	N/A
OR26	7	Full Review Added Appendix A Data Breach Response Plan	Fey Audin	Jan 2020	PSC	N/A
OR26	8	Full Review minor changes	Fey Audin	Dec 2021	QSGC	N/A
OR26	9	Minor word changes Chief Operations Officer to MD. Added Point 1.6 Data Mapping Schedule	Fey Audin	Mar 2023	PSC	N/A

Contributors: Paul Moran
Renewal date: Dec 2023
(This policy has been rebranded for Children's Homes Suite & Schools Suite of policies)

Contents

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
To make 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	**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 2018)

1.2 Fair Ways provides services in education, fostering, training, outreach, contact 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 for Fair Ways to collect personal information in order to carry out its business and provide its services. This includes personal data of service users, employees, contractors and foster carers (present, past and prospective). The information includes name, address, email address, date of birth, contact details 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 is dealt with properly to ensure compliance with the GDPR (2018).

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.

1.5 The lawful basis for collecting personal data is identified as per Article 6 and documented in the Data Mapping Schedule.

2 Scope

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

3 General data protection regulation principles (Article 6)

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'). The legal basis as per Article 6 have been identified and recorded.

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').

4 Information covered by the General Data Protection Regulation

4.1 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.

4.2 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

4.3 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

5 Data protection framework

5.1 The Managing Director has ultimate responsibility for compliance with this policy and the GDPR but has delegated leadership for data protection within Fair Ways 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 Training

GDPR training is core training for all members of staff excluding the maintenance team who do not process personal data and sign a confidentiality agreement.

All new members of staff are provided with the inductees GDPR training within their first three months of working in Fair ways.

As GDPR training is core, there is an expectation for all staff to do an annual refresher GDPR training.

GDPR inductee and refresher training are presented in house and can be booked with the training department training@fairways.co

9 Associated documents & Legislation

- 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]
- GDPR (2018)
- Data Protection (Act 2018)

Appendix A: Data Breach Response Plan

This data breach response plan sets out procedures and clear lines of authority for employees in the event that Fair Ways experiences a data breach [or suspects that a data breach has occurred).

A data breach occurs when company information is lost or subjected to unauthorised access, modification, use or disclosure or other misuse. Data breaches can be caused or exacerbated by a variety of factors, affect different types of information and give rise to a range of actual or potential harms to individuals, agencies and organisations.

This response plan is intended to enable Fair Ways to contain, assess and respond to data breaches in a timely fashion and to help mitigate potential harm to the company or affected individuals. It sets out contact details for the appropriate staff in the event of a data breach, clarifies the roles and responsibilities of staff, and documents processes to assist the Company in responding to a data breach.

A Data Response Team [DRT) has been formed to ensure that all aspects are covered when any breach of data occurs. The Fair Ways DRT consists of the following individuals:

- Data Protection Lead: Paul Moran
- Data Response Team Coordinator: Fey Audin
- Corporate Data Breach Responders: Mac Mchugh, Gareth Webb and Rob Jesson
- Communications Data Breach Responder: Paul Moran
- IT Data Breach Responder: Sean Kitchin
- Departmental Data Breach Responder: Relevant Head of Department

The Data Protection Lead is the main person responsible for managing any breach of data. In periods of absence / annual leave the Data Protection Lead will nominate another individual to manage any breach that occurs. In the absence of the Data Protection Lead the Quality, Safety and Culture team should be informed of any breach so they can direct the breach to the nominated lead.

Following any data breach, the DRT are responsible for considering the below:

- Containing the breach and completing a preliminary assessment
- Evaluating the risks associated with the breach
- Notification
- Preventing future breaches

If Fair Ways experiences a data breach, the below report flow diagram should be followed:
Data breach - report flow diagram

Fair Ways experiences data breach / data breach suspected

- Discovered by Fair Ways Employee or company otherwise alerted

What should the Employee do?

- Employee needs to report the breach / suspected breach to their Line Manager IMMEDIATELY
- Employees should record the time and date the suspected breach was discovered, the type of personal information involved, the cause and extent of the breach and the context of the affected information and breach

What should the Manager do?

- Determine whether a data breach has or may have occurred
- Inform the Data Protection Lead, Paul Moran of the breach providing as much information as possible. If for any reason the Data Protection Lead is not contactable, then please contact the Quality, Safety and Culture team who will be able to direct the breach to the relevant individual who has been nominated by the Data Protection Lead.
- The Data Protection Lead will determine whether the data breach is serious enough to escalate to the Data Breach Response Team or if the breach could be dealt with at manager level. If the breach can be dealt with at manager level the Data Protection Lead will advise the Manager what action should be taken

What should the Data Protection Lead do?

- If the breach cannot be dealt with at manager level the Data Protection Lead will immediately escalate the breach to the Data Breach Response Team
- The Data Protection Lead will inform the Data Breach Co-ordinator of all breaches for recording [those dealt with at manager level and those escalated to the Data Breach Response Team)

Data Response Team				
Co-ordinator	**Corporate**	**Communications**	**IT**	**Departmental**
Fey Audin	Gareth Webb Rob Jesson	Paul Moran	Sean Kitchin	Relevant Director of Department

When should the Data Protection Lead escalate a data breach to the Fair Ways Data Response Team?

The Data Protection Lead is to use discretion in deciding whether to escalate the breach to the DRT. Some data breaches may be comparatively minor, and able to be dealt with easily by the relevant Line Manager and Data Protection Lead without action from the DRT.

For example, a member of staff, as a result of human error, sends an email containing personal information to the wrong recipient. Depending on the sensitivity of the contents of the email, if the email can be recalled, or if the staff member can contact the recipient and the recipient agrees to delete the email, it may be that there is no need to escalate the issue to the response team. In this circumstance the breach has been dealt with at managerial level and the Data Protection Lead should inform the DRT Co-ordinator to record this.

The Data Protection Lead should use their discretion in determining whether a data breach or suspected data breach requires escalation to the response team. In making that determination, the following questions should be considered:

- Are multiple individuals affected by the breach or suspected breach?
- Is there [or may there be) a real risk of serious harm to the Company or affected individual[s)?
- Does the breach or suspected breach indicate a systemic problem in Fair Ways processes or procedures?
- Could there be media or stakeholder attention as a result of the breach or suspected breach?

If the answer to any of these questions is 'yes', then it may be appropriate for the Data Protection Lead to notify the DRT.

Recording of minor breaches

If the Data Protection Lead decides not to escalate a minor data breach or suspected data breach to the DRT for further action an email must be sent to the DRT Coordinator containing the following information:

- Description of the breach or suspected breach

- Action taken by the Data Protection Lead or Fair Ways staff to address the breach or suspected breach
- The outcome of that action and reason the breach was not escalated to the DRT

The Data Response Team Coordinator will record this information on a centralised Data Breach Log.

Data Response Team Process

When the DRT are informed of any data breach, there is no single method of responding. Data breaches must be dealt with on a case-by-case basis, by undertaking an assessment of the risks involved, and using that risk assessment to decide the appropriate course of action.

There are four key steps to consider when responding to a breach or suspected breach.

- **STEP 1**: Contain the breach and do a preliminary assessment.
- **STEP 2**: Evaluate the risks associated with the breach.
- **STEP 3**: Notification.
- **STEP 4**: Prevent future breaches.

The DRT should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession.

The DRT should refer to the below flow chart which provides further details on each step.

Depending on the breach, not all steps may be necessary, or some steps may be combined. In some cases, it may be appropriate to take additional steps that are specific to the nature of the breach.

Records management

Any documents created by the DRT are to be sent to the DRT Co-ordinator to file appropriately.

Internal reporting of data breaches

The Data Protection Lead will include details of any data breach in a quarterly report to the Board of Directors.

STEP 1
Contain the breach and make a preliminary assessment

- Convene a meeting of the DRT
- Immediately contain breach: IT to secure systems if necessary and secure building if necessary
- Inform the Fair Ways Board of Directors and provide ongoing updates on key developments
- Ensure evidence is preserved that may be valuable in determining the cause of the breach, or allowing Fair Ways to take appropriate corrective action
- Consider developing a communications or media strategy to manage public expectations and media interest

STEP 2
Evaluate the risks for individuals associated with the breach

- Conduct an initial investigation promptly and collect information about the breach including the date, time, duration and location of the breach, the type of personal information involved, how the breach was discovered and by whom, the cause and extent, the affected individuals or possible affected individuals, the risk of serious harm to the affected individuals and the risk of other harms
- Determine whether the context of the information is important (to an individual, group or organisation)
- Establish the cause and extent of the breach
- Assess priorities and risks based on what is known
- Keep appropriate records of the suspected breach and actions of the DRT, including the steps taken to rectify the situation and the decisions made

STEP 3
Consider breach notification

- Determine who needs to be made aware of the breach internally and potentially externally at this preliminary stage
- Determine whether to notify affected individuals, consider if there is a real risk of serious harm to the affected individuals. In some cases, it may be appropriate to notify the affected individuals immediately; e.g. Where there is a high level of risk of serious harm to affected individuals
- Consider whether others should be notified, including police / law enforcement or other agencies or organisations affected by the breach or where Fair Ways is contractually required
- Consider if the Information commissioner's Office (ICO) need to be notified in line with GDPR

STEP 4
Review the incident and take action to prevent future breaches

- Fully investigate the cause of the breach
- Report to Fair Ways Board of Directors on outcomes and recommendations
- Update security and response plan if necessary
- Make appropriate changes to policies and procedures if necessary
- Revise staff training practices if necessary
- Consider the option of an audit to ensure necessary outcomes are affected

A. Flowchart showing notification requirements