GLADE School

Confidentiality Policy

(Organisational)

Document Ref:	Version No:	Summary of Changes:	Author:	Release Date:	Approved By:	Lessons learned Ref:
OR26A	1	Full review of policy and split with confidentiality and information sharing	Sarah O'Neil	Feb 2018	QSGC	N/A
OR26A	2	Update changes to responsibilities and wording of legislation to Data Protection Act 2018	Fey Audin	Feb 2019	QSGC	N/A
OR26A	3	Full review	Sean Kitchin	June 2020	QSGC	N/A
OR26A	4	Full review- changes Gareth Webb from COO to MD and replaced Jane Jarvis with Harriett Whitren-Jones.	Sean Kitchin	June 2022	QSGC	N/A
OR26A	5	Amended GDPR to UK GDPR	Fey Audin	June 2023	PSC	N/A

Contributors: Paul Moran, Fey Audin (V1-4)
Review date; June 2024

Contents

Fair Ways Vision, Mission and Values (2024)

Our vision
To build a community that changes lives, makes a difference to society and leaves a legacy greater than ourselves and our contributions.

Our mission
To grow a compassionate, resilient, and trauma-informed community, that embraces learning, so that we improve the lives and outcomes of individuals.

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 that must be observed by all who work for Fair Ways and have access to person-identifiable information or confidential information. All employees need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. This is a requirement of their contractual responsibilities and complies with common law obligations of confidentiality and the Data Protection Act 2018 and General Data Protection Regulations 2018. (UK GDPR)

1.2 Fair Ways provides services in Education, Fostering, Training, Outreach, Health care 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 Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth. This information must not be stored on removable media unless it is encrypted as detailed in the Acceptable Usage Policy (DOC REF OR54)

1.4 Confidential information is anything that is or has been acquired in confidence, relates to Fair Ways business, or that of other persons or bodies whom Fair Ways have dealings and has not been made public. It also includes information about any individual that they would not expect to be shared. Confidential information can take many forms including employee records, occupational health records, business information and information relating to service users.

1.5 Information can relate to service users and employees (including temporary employees), however stored. Information may be held on paper, USB sticks or any form of computerised storage or even heard by word of mouth.

1.6 A summary of Confidentiality Do's and Don'ts can be found in Appendix A.

1.7 A summary of the regulatory framework for confidentiality which forms the key guiding principles of this policy can be found in Appendix B.

1.8 How to report a breach of this policy and what should be reported can be found in Appendix C.

2 Scope

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

3 Roles and responsibilities

3.1 **Gareth Webb (Managing Director)** has overall responsibility for strategic and operational management, including ensuring that Fair Ways' policies comply with all legal, statutory and good practice guidance requirements.

3.2 **Paul Moran (Director of IT & Communications)** will facilitate the development and implementation of Information Governance within Fairways. They are responsible for the review of this policy, providing advice on request to any employee on the issues covered within it, and ensuring that training is provided for all employee groups to further their understanding of the principles and their application.

3.3 **The Quality, Safety and Governance Committee** ensures that Fair Ways is meeting its obligations under national, regional and local service user safety experience standards and that statutory and regulatory standards are met.

3.4 **Harriett Whitren-Jones (Director of Human Resources Operations)** is responsible for ensuring that the contracts of all employees (permanent and temporary) are compliant with the requirements of this policy and that confidentiality is included in induction training for all employees.

3.5 **Directors and Managers** are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. They must ensure that any breaches of the policy are reported in line with the Data breach response plan (Appendix D).

3.6 **All Employees** need to be aware of their responsibilities for safeguarding confidentiality and preserving information security. This is a requirement of their contractual responsibilities and complies with common law obligations of confidentiality, the Data Protection Act 2018 and the General Data Protection Regulations (UK GDPR).

3.6.1 Any breach of confidentiality, inappropriate use of employee records, service user or business sensitive / confidential information, or abuse of computer systems is a

disciplinary offence, which could result in dismissal or termination of employment contract and must be reported.

4 Principles

4.1 All employees must ensure that the following principles are adhered to

- Person-identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of.
- Access to person-identifiable or confidential information must be on a need-to-know basis.
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required.
- Recipients of disclosed information must respect that it is given to them in confidence.
- If the decision is taken to disclose information, that decision must be justified and documented.
- Any concerns about disclosure of information must be discussed with either the relevant line manager or the information governance lead.

4.2 Fair Ways is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

4.3 Person-identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the facts of the data.

4.4 Person-identifiable or confidential information is stored in various formats and locations. In mixed office environments measures should be in place to prevent oversight of person-identifiable information by unauthorised parties and should be appropriately stored.

4.5 All employees should adopt a clear desk policy at the end of each day. In particular employees must keep all records containing person-identifiable or confidential information in recognised filing, within lockable storage.

4.6 Unwanted printouts containing person-identifiable or confidential information must be shredded. Discs, tapes, printouts and fax messages must not be left lying around but be filed and locked away when not in use.

5 Disclosing personal / confidential information

5.1 To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

5.2 It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

5.3 For more information about disclosing personal / confidential information please see the Information Sharing Policy (DOC REF OR26B).

6 Breaches

6.1 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

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

6.3 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) and Password Management Policy (DOC REF IT08)

6.4 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 D) 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.

6.5 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

7 Associated documents & Legislation

- Data protection policy [DOC REF OR26]
- Consent, privacy notices & individual rights Policy [DOC REF 26A]
- Information sharing policy [DOC REF OR26B]
- Acceptable usage policy [DOC REF OR54]
- Social media policy [DOC REF OR78]
- Password management policy [DOC REF IT08]
- Data Protection Act 2018
- Information sharing: advice for practitioners providing safeguarding services (July 2018)
- Working Together 2015
- The Data Protection Act 2018
- The General Data Protection Regulations (UK GDPR 2018)
- Caldicott Guardian Principles
- The Care Act 2014
- Common law duty of confidentiality

Appendix A - Confidentiality Dos and Don'ts

(This is not an exhaustive list)

Dos

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with.
- Do ensure visitors are signed in and out and accompanied in areas containing personal and sensitive information.
- Do clear your desk at the end of each day, locking away any portable records containing person-identifiable or confidential information.
- Do be mindful not to give service users access to previously saved addresses when using company SATNAVs
- Do switch off computers with access to person-identifiable or business confidential information, or lock them, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do ensure doors and fire exits are secure when leaving a building and that codes for key safes are kept safe and changed when necessary.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely, when necessary, as per the Information Sharing Policy (DOC REF OR26B) and the Acceptable Usage Policy (DOC REF OR54).
- Do report any actual or suspected breaches of confidentiality.

Don'ts

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B – Summary of regulatory framework

Fair Ways provides services in Education, Fostering, Training, Outreach, Health care and Residential care for children and adults. Fair Ways collects and retains data on employees, foster carers and service users within these services. These services are regulated under differing legislations.

Fair Ways shall comply with the following legislation and guidance as appropriate:

- Information sharing: advice for practitioners providing safeguarding services (July 2018)
- Working Together 2015
- The Data Protection Act 2018
- The General Data Protection Regulations (UK GDPR 2018)
- Caldicott Guardian Principles
- The Care Act 2014
- Common law duty of confidentiality

Further details of the guidance can be found at the following links:

https://www.gov.uk/government/publications/safeguarding-practitioners-information-sharing-advice

For Children:

http://4lscb.proceduresonline.com/hampshire/p_info_sharing.html#gov_guidance

For Adults:
https://www.southampton.gov.uk/Images/Multi-Agency-Safeguarding-Adults-Policy-and-Guidance-2nd-Edition-December-2016_tcm63-372918.pdf

Appendix C - Reporting of policy breaches

What should be reported?

Misuse of personal data and security incidents must be reported so that steps can be taken to rectify the problem and to ensure that the same problem does not occur again.

All confirmed breaches should be reported to the information governance lead. If employees are unsure as to whether a particular activity amounts to a breach of the policy, they should discuss their concerns with their line manager or the information governance lead.

The following list gives examples of breaches of this policy which should be reported:

- Sharing of passwords.
- Unauthorised access to Fair Ways systems either by employees or a third party.
- Unauthorised access to person-identifiable information where the employee does not have a need to know.
- Disclosure of person-identifiable information to a third party where there is no justification and there are concerns that it is not in accordance with the DPA, UK GDPR or the Fair Ways Confidentiality Policy.
- Sending person-identifiable or confidential information in a way that breaches confidentiality.
- Leaving person-identifiable or confidential information lying around for anyone passing to see.
- Theft or loss of person-identifiable or confidential information.
- Disposal of person-identifiable or confidential information in a way that breaches confidentiality i.e., disposing off person-identifiable information in a normal waste bin.

Seeking Guidance

It is not possible to provide detailed guidance for every eventuality, therefore, where further clarity is needed, please speak to your line manager or the information governance lead. Once a breach is reported the organisation Data breach response plan (Appendix D) will be followed.

Appendix D - 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 manager 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 UK 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