



Fair Ways Education

(Organisational)

Information Sharing Policy

Document Ref:	Version No:	Summary of Changes:	Author:	Release Date:	Approved By:	Lessons learned ref
OR26B	1	Full review of policy and split with confidentiality and data protection policies	Sarah O'Neil	Feb 2018	QSGC	N/A
OR26B	2	Review changes to responsibilities	Fey Audin/Sarah O'Neil	March 2019	QSGC	N/A
OR26B	3	Full review minor word changes	Fey Audin	June 2020	QSGC	N/A
OR26B	4	Full review: changes to wording in section 5 to reflect use of links to Share Point and On Drive files.	Fey Audin	July 2022	QSGC	N/A

Contributors: Paul Moran, Sean Kitchin
Renewal Date: July 2024



Contents

1	Introduction	4
2	Scope.....	4
3	Sharing Information	5
4	Principles.....	5
5	Procedures	7
6	Associated documents & Legislation	8



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*:

P ROFESSIONAL	A CCEPTING	R ELECTIVE	T RANSPARENT
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 as part of their role are required to share person-identifiable information or confidential information. All employees need to be aware of their responsibilities with regards to sharing information within the organisation and with third parties.
- 1.2 As Fair Ways provides a variety of services for children, young people and families, all children, young people and adults will be referred to in this policy as 'service users' for ease of reference.
- 1.2 Person-identifiable information is anything that contains the means to identify a person for example: name, address, postcode, date of birth, contact numbers, National Insurance number, passport number, credit / debit card number etc.
- 1.3 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.
- 1.4 Information can relate to service users and employees (including temporary employees), however stored. Information may be held on paper, or any form of digital storage or even heard by word of mouth.
- 1.5 Effective information-sharing plays an intrinsic part of the services that Fair Ways provides, as multiple agency working is vital when providing care for our service users. There is a need to share information across organisational and professional boundaries, in order to ensure effective co-ordination and integration of services.
- 1.6 The Government has emphasised the importance of security and confidentiality in relation to personal information and the sharing of this and has strengthened the legislation and guidance in this area through the Data Protection Act (DPA) 2018 and the General Data Protection Regulation 2018(GDPR) .

2 Scope

- 2.1 All Fair Ways employees, contractors and foster carers are within the scope of this policy. This includes permanent employees, temporary employees, bank employees and employees of subsidiary companies.

3 Sharing Information

3.1 Information sharing, in the context of this policy, means the disclosure of personal information from Fair Ways to a third-party organisation or information shared internally within Fair Ways. Information sharing can take the form of:

- a reciprocal exchange of data
- providing data to a third party or parties
- several organisations pooling information and making it available to each other
- several organisations pooling information and making it available to a third party or parties
- exceptional, one-off disclosures of data in unexpected or emergency situations

3.2 *"Effective sharing of information between professionals and local agencies is essential for effective identification, assessment and service provision.*

Early sharing of information is the key to providing effective early help where there are emerging problems. At the other end of the continuum, sharing information can be essential to put in place effective child protection services. Serious Case Reviews (SCRs) have shown how poor information - sharing has contributed to the deaths or serious injuries of children.

Fears about sharing information cannot be allowed to stand in the way of the need to promote the welfare and protect the safety of children." (Working Together 2015)

4 Principles

4.1 The principles set out below are intended to help employees working in Human Resources and with service users to share information internally and with third parties.

4.2 These principles are derived from the seven highlighted key principles made by the Caldicott report, which was a report produced by Dame Fiona Caldicott, who chaired a committee to review increasing worries concerning the use of patient information in the NHS in England and Wales and the need to avoid the undermining of confidentiality because of the development of information technology, and its ability to propagate information concerning patients in a rapid and extensive way. These principles should underpin information governance across all health and social care services.

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for services users/ employees to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

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. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data are made fully aware of their responsibilities and obligations to respect service user's and employees' confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect service user's confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies

- 4.3 Information sharing decisions should be recorded whether the decision is taken to share or not. If the decision is to share, reasons should be cited including what information has been shared and with whom. If the decision is not to share, it is

good practice to record the reasons for this decision and discuss them with the requester.

- 4.4 Employees should use their judgement when making decisions on what information to share and should consult with their manager if in doubt. The most important consideration is whether sharing information is necessary to safeguard and protect a service user / employee.

5 Procedures

5.1 Sharing information over the telephone

- 5.1.1 Before any personal information is shared over the telephone, employees must ensure that they know whom they are speaking to and that the sharing of information is necessary and relevant. If in doubt, employees should take the caller's name and telephone number and carry out checks with relevant colleagues / line manager or check in service user records if information should be shared before calling back.

5.2 Sharing information via email

- 5.2.1 All emails sent from Fair Ways employees should contain the following disclaimer:

***Email Disclaimer:** This email and any files transmitted with it may contain information which is privileged and confidential, the disclosure of which is prohibited by law and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please note any dissemination, distribution or copying of this message is strictly prohibited. Please notify the sender immediately if you have received this email by mistake and delete it from your system. Email transmissions cannot be guaranteed to be secure or error-free as information can be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses The sender therefore does not accept liability for any errors or omissions in the contents of this message.*

Fair Ways is the trading name of the charity, Fair Ways Community Benefit Society, registration number 8691"

- 5.2.2 When sending personal data about a service user/ employee , use initials rather than full names where appropriate.
- 5.2.3 No confidential or sensitive information should be included in the body of email.

5.2.4 Methods to be used when sharing confidential or sensitive information via email:

- Send the One Drive / Share Point folder link to the document to the relevant person.
- When attaching a document to an email it must be password protected.
- Password to be communicated verbally either via phone or Teams and not via email.
- Ensure password is recorded for future reference.
- Encrypt email by typing 'encrypt' as the first word in the subject line.

(Contact the Data Protection Coordinator fey.audin@fairways or IT IT@fairways.co for guidance on how to: password protect a document; share a One Drive / Share Point folder link; and to encrypt an email.)

5.2.4 Where an email must be used to transmit confidential information exercise caution and always check the following before sending:

- Check that the email address you are sending to, is correct.
- Check that the correct attachment has been attached.
- Check if attachment has been password protected.
- Check that 'encrypt' is in the subject line.
- Where necessary request confirmation of safe receipt

5.3 **Sharing information via mobile storage device**

5.3.1 Fair Ways has disabled the use of all third-party storage devices. In rare circumstances, the organisation may authorise the use of a third-party storage device, on an individual basis, where no other options are available. Only Fair Ways authorised equipment may be used.

6 **Associated documents & Legislation**

- Confidentiality Policy [DOC REF OR26A]
- Data Protection Policy [DOC REF OR26]
- Acceptable Usage Policy [DOC REF OR54]
- Data Protection Act (2018)