Data Sharing Policy

Document Owner:	CFL
Version:	Version 1.1
Approved Date:	06/03/24
Review Date:	March 2025

Change history

Date	Version	Created by	Description of change
16/2/2023	V1	M Mirza (Moore ClearComm)	Initial draft
06/03/24	V1.1	C Fulton-Langley	2024 version

Table of contents

1. Introduction

1.1 This policy covers all activities of the Future Men, where personal data is disclosed or shared with another organisation and which disclosing / sharing must comply with the requirements of the Data Protection Act 2018 ('DPA 2018') and the UK General Data Protection Regulation ('UK GDPR').

1.2 The UK GDPR and the DPA 2018 do not prevent personal data being shared where it is appropriate to do so. Sharing or disclosing personal data is permissible but it must be done in compliance with the data protection legislation and specifically the Information Commissioner's statutory Data Sharing Code of Practice ('the Code').

1.3 Data sharing can include sharing personal data on a routine, regular basis with another organisation or it can be one off or ad-hoc disclosures of personal data. It is also important to consider the risks of not sharing personal data and so training and awareness of this policy amongst staff is important.

1.4 A list of terms and definitions used in the UK GDPR is at Annex A.

2. Scope

2.1 This policy applies to all directors, trustees, employees, consultants, and contractors, (hereafter 'staff') who use or remotely access Future Men systems or information, either occasionally or as part of an ongoing agreement. It applies to information in all formats, including manual records and electronic data.

2.2 The policy covers security which can be applied through the appropriate technology but perhaps more crucially, it encompasses the behaviour of the people who manage information in the line of Future Men's business activities.

3. Policy Statement

3.1 Future Men is committed to compliance with all relevant UK laws in respect of personal data and to the protection of the "rights and freedoms" of individuals whose information has been collected and processed in accordance with the UK GDPR and DPA 2018.

3.2 Future Men is under a lawful obligation to ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police and other law enforcement agencies.

3.3 Staff should exercise caution when asked to disclose personal data held on another individual to a third party and will be required to attend specific training that enables them to deal effectively with the risks associated with any such disclosure of personal data.

3.4 Notwithstanding the foregoing, it should be borne in mind that the disclosure of personal data may be relevant to, and necessary for, the conduct of the business and so it is important that staff are properly trained to deal with any requests appropriately.

3.5 This policy applies to all Future Men staff wherever they work. Any breach of the UK GDPR or DPA 2018 may be dealt with under Future Men's Disciplinary Policy.

3.6 The requirements of the UK GDPR, DPA 2018 and this policy apply to all disclosures of personal data relating to staff, clients, customers, and service users.

4. Roles and Responsibilities

4.1 Future Men is the data controller as defined in the UK GDPR.

4.2 The Board and all those in managerial or supervisory roles throughout Future Men are responsible for developing and encouraging good information handling practices within their respective areas of responsibility.

4.3 The CEO is responsible for data protection matters within Future Men. For the purposes of this policy, the responsible person will be the point of contact for staff with any queries.

4.4 Compliance with data protection legislation is the responsibility of all staff who process personal data.

4.5 Future Men's new joiner and induction process sets out specific training and awareness requirements in relation to specific roles and staff generally.

5. Data Sharing Code of Practice

5.1 The Data Sharing Code of Practice ('the Code'), issued by the Information Commissioner, provides practical advice to businesses and organisations on how to carry out responsible data sharing in compliance with data protection law and aims to give data controllers the confidence needed to share data lawfully, fairly, and proportionately. Accordingly, the Code provides advice on:

- Data Protection Impact Assessments ('DPIAs');
- data sharing agreements;
- data protection principles;
- due diligence;
- data sharing and children;
- data sharing in an urgent situation or an emergency;
- lawful basis for sharing personal data;
- law enforcement processing.

6. Data Sharing

6.1 Data sharing is not defined in the legislation, but the Code issued by the Information Commissioner covers the 'disclosure of personal data by transmission, dissemination or otherwise making it available'.

6.2 This policy (and the Code) does not apply to the internal sharing of personal data (i.e. within the organisation) or to the sharing of personal data with data processors. A sharing relationship with a data processor will need to be dealt with under a separate process and covered by a data processing agreement.

6.3 In practice, this means that this policy covers:

- sharing or disclosing personal data with a third party (external organisation) on a routine/regular basis. This will mean the same type of data is shared regularly, is necessary, and for an agreed and established purpose
- an exceptional, one-off disclosure of personal data that is ad hoc or required urgently or in an emergency.

7. Routine Data Sharing

7.1 For routine and regular data sharing with an external organisation/s, staff will need to ensure that appropriate safeguards are in place. These will include:

- Undertaking a DPIA beforehand if the processing is likely to result in a high risk to the rights and freedoms of individuals. The Information Commissioner's advice is to undertake a DPIA even it is not high risk as the process assists in identifying any risks with the processing.
- Staff will need to ensure that the data sharing is necessary, proportionate, and lawful as well as ensuring that it complies with the relevant data protection principles.
- A Due Diligence Questionnaire (DDQ) should be completed by the other party/parties to the data sharing arrangement to ensure that adequate protections are in place to protect the personal data being shared. There is a reputational risk if due diligence is not applied.
- Staff are to ensure that a Data Sharing Agreement (DSA) is in place prior to undertaking any routine disclosures of personal data. Although a DSA is not mandatory, it is good practice and substantially reduces any risks of non-compliance. It also ensures the organisation has appropriate governance in place, so it is clear what personal data is being disclosed, why and to whom. A DSA, amongst other things, include:
    - the parties to the agreement;
    - the purposes for the processing;
    - the personal data being shared and how it will be shared;
    - the lawful basis for the sharing;
    - what information governance will be put in place;
    - the period for which the sharing will occur;
    - what will happen to the personal data at the end of the arrangement; and
    - how data subject rights will be handled.

7.2 There should be a central log of data sharing arrangements/agreements so that there is appropriate oversight and that the arrangements are kept under review to ensure that the sharing continues to be effective, justified, and necessary.

7.3 For those arrangements where you are allowing a third party to have access to your IT systems for the purposes of sharing personal data, this will require more rigorous scrutiny as well as security/IT checks. In these circumstances a DPIA should be undertaken as a first step, supported by an appropriately worded DSA.

8. Non-Routine Disclosures

8.1 Requests for one-off disclosures of personal data can come into the organisation in different ways and therefore staff need to be aware of what they need to do when they receive these requests.

8.2 For non-routine/ad hoc or one-off requests for personal data there will often be no time to undertake a thorough assessment in order to reach a decision about the disclosure. Accordingly, this policy sets out what needs to be done in those circumstances to ensure staff make appropriate decisions. Staff must be trained on these processes as the risks can be that personal data is disclosed when it should not have been or that personal data is not shared when it should be.

8.3 The member of staff receiving the request will need to consider:

- who is asking for the information?
- has the name, position, organisation, and contact details of the person asking for the information been recorded?
- has the identity of the person requesting the information been verified?
- what information is being requested?
- for what purpose will it be used?
- is personal information being requested?
- does a statutory or common law provision exist, and has a policing purpose to share information been established?
- if yes, in what format does the requester want the information?
- when does the requester want the information?

8.4 Circumstances permitting, the person seeking the disclosure of personal data held by Future Men should be asked to submit a 'Disclosure Request Form' (Annex B). In circumstances where the requester is not able to complete the 'Disclosure Request Form', it should be completed on their behalf by the member of staff handling the disclosure request on behalf of Future Men.

8.5 Requests from law enforcement agencies e.g. the police, for the disclosure of personal data held by Future Men will ordinarily be made using the requester's request form. The disclosure of personal data in these circumstances will be for a policing purpose.

8.6 It is for Future Men, acting in the capacity of a controller, to decide whether information is to be disclosed to a law enforcement agency. The only time the request must be complied with is if Future Men is legally required to disclose information under a court order.

8.7 Staff will need to be clear when it will be appropriate to share personal data, but each request will need to be considered on its own merits. Examples of where a disclosure might be necessary may include:

- where children or vulnerable adults are at risk of harm
- where there is a risk of physical harm to an individual
- a public health emergency
- preventing a loss of life
- reasons of national security.

8.8 Decisions relating to the disclosure of the personal data should be documented, including the legal basis for the disclosure. This may be done after the disclosure particularly if the decision is made in relation to an emergency situation, but nonetheless any decision making needs to be documented outlining the reasons for the disclosure.

8.9 Consideration will need to be given to the consequences of not sharing personal data.

8.10 Advice should be sought from the CEO as appropriate.

9. Transparency

9.1 It is important that data subjects are aware that personal data about them may be shared as individuals have a right to be informed (Article 13 of the UK GDPR). Future Men's privacy notices contain details of the instances where personal data will/may be shared.

10. Security

10.1 All staff are responsible for ensuring that any personal data which Future Men holds and for which it is responsible is kept secure and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised to receive the personal data.

10.2 New directors and staff members, at all levels, as part of their induction process, are given guidance on where these documents can be found on the shared drive/intranet.

11. Personal data breaches

11.1 Any loss or suspected loss, or any unauthorised or suspected unauthorised disclosure of personal data must be reported in accordance with the 'Personal Data Breach Policy'.

11.2 Personal data breaches may need to be reported to the ICO.

12. Disciplinary Action

12.1 All staff are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct.

12.2 Future Men reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with Future Men.

Annex

A – UK GDPR Definitions
B – Disclosure Request Form

Annex A – UK GDPR Definitions

Child – in the United Kingdom of Great Britain and Northern Ireland, the processing of personal data of a child under the age 13, in relation to 'Information Society Services', is only lawful if the consent of the person with parental responsibility has been obtained. The controller shall make reasonable efforts to verify that consent is given or authorised by the person who is the holder of parental responsibility over the child.

Data controller – the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data subject consent - means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Personal data – 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.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party – a natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Annex B – Disclosure Request Form

[Section 1 and 2 to be completed by the requester]

Section 1 – Details of Requester

Requester:	
Job Title:	
Organisation:	
Address:	
Telephone:	
Secure email address:	
Date:	

Section 2 – Details of Data Subject

Name	
Address	
Other identifying information such as date of birth	
What personal data is being requested and why is it necessary?	
When is the personal data required?	

Section 3 – To be completed by Future Men

Does the organisation hold the personal data being requested?	
Is there a legal basis to justify the disclosure? If so, what is it?	
Does the organisation need to tell the data subject?	
How will the personal data be disclosed – secure email, post or in person?	

Section 4 – Review and approval

APPROVAL	NAME/TITLE	DATE
Disclosure approved by:		
Disclosure made by:		