Data Protection Policy Statement

1 WHY THIS POLICY EXISTS

Ford Forward Community Chaplaincy (Ford Forward) is committed to a policy of protecting the rights and privacy of individuals (including team members, clients and others). We need to process and retain certain information about our team and clients and other individuals we have dealings with for administrative purposes and to record progress. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

In addition Ford Forward must adhere to the Prison Service Data Protection Policy in relation to Prison Service data.

- As a matter of good practice, other agencies and individuals working with Ford Forward and who have access to personal information will be expected to have read and comply with this policy. It is expected that those who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

2 BACKGROUND TO DATA PROTECTION

Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge and, wherever possible, is processed with their consent.

All mentoring relationships aim to be open and honest, so it is important that clients understand what we are recording about them and why. Mentors should be mindful of what they record about the mentee. Nothing should be recorded that the mentor is not happy to share with the client.

3 DEFINITIONS (TAKEN FROM THE DATA PROTECTION ACT 1998)

Personal data
Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number and ID number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive data
Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data is subject to much stricter conditions of processing.

Data controller
Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which the personal data is processed.

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

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes obtaining and recording data, accessing, altering, adding to, merging, deleting data, retrieval, consultation or use of data, disclosure or otherwise making available of data.

Third party

Any individual/organisation other than the data subject, the data controller or its agents.

Relevant filing system

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. Please note that this is the definition of relevant filing system in the Act. Personal data as defined and covered by the Act can be held in any format, electronic (including websites and e-mails), paper-based, photographic, etc from which the individual's information can be readily extracted.

4 RESPONSIBILITIES

Ford Forward, as a corporate body, is the data controller. Compliance with data protection legislation is the responsibility of all members of our team. We are all responsible for ensuring that any personal data held is accurate and up to date.

NOTIFICATION

Notification of data breaches is the responsibility of the Trustees. Details for notifications are at http://www.informationcommissioner.gov.uk.

Data breaches must be notified to the Trustees as soon as known and, in any event, within 72 hours. The Treasurer is primarily responsible for reporting data breaches.

5 DATA PROTECTION PRINCIPLES

All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully - Those responsible for processing personal data must ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept. *This is covered in the Consent Form.*
2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes - Data obtained for specified purposes must not be used for a purpose that differs from those.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held - Information which is not strictly necessary for the purpose for which it is obtained should not be collected. If data is given or obtained which is excessive for the purpose, it should be immediately deleted or destroyed. *E.g. data relating criminal record must not be held.*
4. Personal data shall be accurate and kept up to date. No data should be kept unless it is reasonable to assume that it is accurate. It is the responsibility of individuals to ensure that data held is accurate and up to date. Completion of the Consent Form will be taken as an indication that the data contained therein is accurate. Individuals should update personal records accordingly. *E.g. sharing assessment scores with the data owner, their own and ours, and agreeing the outcome of the meeting with them at its conclusion, together with the action plan, so that everything we hold is open and with the data owner's consent.*
5. Personal data shall be kept not be kept for longer than 12 months, unless a new Consent Form has been completed and signed.
6. Personal data shall be processed in accordance with the rights of data subjects - see section 5 below.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data. *Tablets and laptops used to access data will be encrypted. Access codes to iizuka must not be held electronically.*
8. Personal data shall not be transferred to a country or territory outside the United Kingdom without the explicit consent of the individual. Team members should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the globe.

6 DATA SUBJECT RIGHTS

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of any automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by an automated process
- To sue for compensation if they suffer damage by any contravention of the Act
- To take action to rectify, block, erase or destroy inaccurate data
- To have data removed
- To request the Information Commissioner to assess whether their rights have been contravened

7 CONSENT

Personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent. Ford Forward understands consent to mean that the data subject has been fully informed of the intended processing and has signified their agreement by completing and signing a Consent Form, whilst being in a fit state of mind to do so and without pressure being exerted upon them - the individual must sign the form freely of their own accord.

Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

The Consent Form contains a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe, e.g. if a published testimony contains personal data. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place, i.e. data can only be used for the specific purpose agreed at the time of signing of the Consent Form.

8 PRISON SERVICE DATA

Of necessity all prison service data is closely controlled, and any data leaks will be highly sensitive. To avoid any potential conflicts, Ford Forward will only store data which is freely available and given by the client. It should be also be possible to prove that all data stored is given in this way by use of suitable referral or assessment documentation.

To avoid conflicts and debates on ownership, any data stored electronically by Ford Forward will NOT be stored on a prison service computer.

9 SECURITY OF DATA

Each team member is responsible for ensuring that any personal data (on others) which they hold is kept securely and that it is not disclosed to any unauthorised third party (see section on disclosure of data for more details).

All personal data should be accessible only to those who need to use it, e.g. the code reference for individuals is not shared with the wider team. You should form a judgement based upon the sensitivity and value of the information in question, but always keep personal data:

- in a lockable room with controlled access
- in a locked drawer or filing cabinet
- if computerised, password-protected and on an encrypted machine
- anonymised by the use of numeric references in place of names

Do not:

- downloaded from iizuka, other than in anonymised report format
- store links or shortcuts to iizuka
- store log-ins or passwords on the machine you use to access data
- store data on disk

Care should be taken to ensure that PCs and terminals are not visible to others and that computer passwords are kept confidential. PC screens should not be left unattended without password-protected screen-savers and manual records should not be left where others can access them.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as confidential waste. Hard drives of redundant PCs should be disposed of appropriately.

Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. As Ford Forward will generally process personal data off-site, team members should take particular care when processing personal data.

10 RIGHTS OF ACCESS TO DATA

Clients have the right to access any personal data which is held in electronic format and manual records which form part of a relevant filing system.

Any individual who wishes to exercise this right should apply in writing to the Trustees.

Any such request will normally be complied with within 30 days of receipt of the written request.

11 DISCLOSURE OF DATA

The team must ensure that personal data is not disclosed to unauthorised third parties; this includes family members, friends, other government bodies and, in certain circumstances, the police. We should all exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's Ford Forward contact details in response to an enquiry regarding something for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work-related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to and necessary for the conduct of normal business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the person concerned.

This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- the individual has given consent (e.g. a team member/client has consented to the project corresponding with a named third party)
- where the disclosure is in the legitimate interests of Ford Forward (e.g. disclosure to team members – personal information can be disclosed to other team members if it is clear that they require the information to enable them to perform their jobs)
- where disclosure of data is required for the performance of a contract

Certain disclosures are permissible without consent so long as the information is requested for one or more of the following purposes:

- to safeguard national security
- prevention or detection of crime, including the apprehension or prosecution of offenders
- assessment or collection of tax duty
- discharge of regulatory functions (includes health, safety and welfare of persons at work)
- to prevent serious harm to a third party
- to protect the vital interests of the individual (this refers to life and death situations)
- requests must be supported by appropriate paperwork, e.g. a written record of the circumstances , actions taken and data disclosed sent to the Trustees within 72 hours

12 DATA PROTECTION RISKS

This policy helps to protect Ford Forward and its team from significant data security risks, including:

- **Breach of confidentiality**, e.g. information being given out inappropriately
- **Reputational damage**, Ford Forward could lose the trust of its clients if their data was not considered to be sufficiently secure

Signed on behalf of the Trustees:	
Name of Trustee:	**Mike Peachey**
Date of approval by the Trustees:	**6 June 2018**
Date of First Review	**2 February 2018**
Date of Second Review	**20 September 2019**
Date of Next Review	**20 September 2020**