Data Protection and Records Management Policy

Policy Lead	Fran Kyprianou
Authors	Florence Governance Team
Ratified	Florence Leadership Team 19th January 2024
Policy Number	FNI04
Version Number	1.0
Date of issue	30th January 2024
Date to be reviewed	30th January 2027
The controlled version of this document is stored on the Policy Portal on Notion. **Not controlled once printed**	

Table of Contents

1. Introduction

Information governance is an accountability and decision making framework put in place to ensure that the creation, storage, use, disclosure, archiving and destruction of information is handled in accordance with legal requirements and to maximise operational efficiency. It includes the processes, roles, policies and standards that ensure the compliant and effective use of information in enabling an organisation to achieve its goals.

This policy is important because it will help the people who work for Florence to understand how to look after the information they need to do their jobs, and to protect this information on behalf of users and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management. This Policy establishes the key high-level principles of Information Governance at Florence and sets out responsibilities and reporting lines for members of staff. It provides an overarching framework for Information Governance across Florence.

1. Policy Statement

Florence is fully committed to and compliant with the requirements of the General Data Protection Act 2018 (UK GDPR), Privacy & Electronic Communications (EC Directive) Regulations 2003 (PECR). The company will therefore follow procedures that aim to ensure that all individuals who have access to any Personal Data held by or on behalf of the company are fully aware of and abide by their duties and responsibilities under the above Act and regulations.

Florence regards the lawful and correct treatment of Personal Data as essential to its successful operations and to maintaining confidence between the company, its employees, clients and temporary workers. The company will therefore ensure that it treats Personal Data lawfully and correctly. To this end the company fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018 and UK General Data Protection Regulations as detailed below.

Florence is registered in the register of data controllers with the Information Commissioner's Office (registration number ZA550052) and this registration is renewed on an annual basis.

We have a detailed Data Protection and Privacy Policy and also have and maintain a valid and current Cyber Essentials Certificate which demonstrates how we guard against cyber threats including but not limited to:

- Operating a secure internet connection.
- Ensuring devices and software have security provision.
- Controlling access to our data and services.
- Protecting our equipment and software from viruses and other malware.
- Keeping our devices and software up to date.

2. Scope

In order to operate efficiently, Florence has to collect and use information about the people with whom it works.

Personal Data must be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the UK GDPR to ensure this.

This Policy applies to all staff and agents of Florence, including any users who are processing personal data by third parties acting on behalf of Florence. They are required to comply with this policy, and with the policies and processes that sit under it as part of the information governance framework.

All employees are made fully aware of this policy and of their duties and responsibilities under the UK GDPR.

3. Definitions, Roles and Responsibilities

CEO (Chief Executive Officer) The CEO is ultimately responsible for the overall management and direction of the company. The CEO has the ultimate responsibility for setting the tone and culture for the organisation, ensuring that all employees understand the policy's importance, and overseeing its implementation. Ensuring that systems are in place to support compliance with data protection law. Ensuring that Florence has an appropriate DPO in post, and to ensure that they have adequate resources, freedom and authority to perform

those roles.

Central Team - All direct employees of Florence that are not care professionals working through the Florence platform. Processing personal data in accordance with this policy - as well as other related policies, processes and guidance - to comply with data protection law and to appropriately protect the privacy, rights and freedoms of data subjects.

Service User - a person who uses health and/or social care services. Sometimes known as a "patient", "client" or "person in care".

Care Professionals - Anyone on the Florence platform that carries out work on behalf of Florence in other organisations, for example registered nurses and care assistants.

Employees - everyone employed by Florence directly and indirectly, including care professionals using the platform and the central team.

The Data Protection Officer is responsible for ensuring the implementation of this policy on a day-to-day basis; however, all employees have a responsibility to accept their personal involvement in applying it and must be familiar with the policy and ensure that it is followed by both themselves and employees for whom they have a responsibility.

Disciplinary action may be taken against any employee who acts in breach of this policy. Disciplinary action may include summary dismissal in the case of a serious breach of this policy or repeated breaches. In other cases, it may include a verbal or written warning. Such action will be taken in accordance with the Company's disciplinary procedure.

Breaches of this policy may also result in the employee responsible being held personally liable for compensation if legal action is taken in relation to data protection.

Personal data is any information processed by Florence which identifies and relates to a living person. This includes information which directly identifies a living person, but also to information which is not directly identifiable but which could be linked back to the person by reference to other information which is held by Florence, is likely to come into the possession of Florence, or which Florence has powers to obtain

Data Subjects are the people to whom personal data relates.

Data protection law is any legislation (including Act, regulation or statutory instrument) currently in force which directly applies to the processing of personal data by Florence.

The principal legislation at the time of publication of this policy are the General Data Protection Regulation (GDPR) and the Data Protection Act 2018**.**

Processing means any operation, action on, or interaction with personal data, whether carried out by a person or by automated means.

Processing includes, but is not limited to: access to, obtaining, recording, organisation or structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, sharing, publication, restriction, erasure or destruction of personal data.

Privacy notices are information that is communicated to data subjects to inform them of how and for what purpose(s) their personal data will be processed by Florence, and which provide them with further information prescribed under data protection law, including information of the security and retention of the data, and on the data subject's rights.

4. Procedures

The Principles of Data Protection

We adhere to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).
2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).
4. Accurate and where necessary kept up to date (Accuracy).

5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).
6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).
7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).
8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and can demonstrate on request compliance with the data protection principles listed above.

Lawfulness, Fairness & Transparency

Personal Data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

We will only collect, process and share Personal Data fairly and lawfully and for specified purposes. The Data Protection Legislation restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject. The Data Protection Legislation allows Processing for specific purposes, some of which are set out below:

- The Data Subject has given his/her Consent;
- The Processing is necessary for the performance of a contract with the Data Subject;
- To meet our legal compliance obligations;
- To protect the Data Subject's vital interests; or
- To pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental

rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests are set out in our Privacy Policy.

You must identify and document the legal ground being relied on for each Processing activity. We have already identified and documented the grounds for the lawful Processing of Personal Data.

Individuals Right to Data Protection Law

Florence will also comply with the other requirements of data protection law, which include, but is not limited to:

Providing privacy notice to inform data subjects as to how and why we may process their personal data, and as to their rights.

- Florence will produce and publish 'privacy notices' which we shall make available on our website and, where appropriate, in other Florence publications.
- Where we collect personal data directly from data subjects (e.g. on forms, webforms or surveys, or when asking for information in person or via electronic communications) we will provide a privacy notice at the point of collection.
- When we collect personal data via a third party, we will ensure that a privacy notice is communicated to the data subject to the extent that it is proportionate and reasonable in the circumstances to do so.

Complying with the rights of data subjects

Florence will ensure that there are processes in place to comply with the rights of data subjects. These include:

- **Right of data access:** Florence will have a process to manage and respond to requests from data subjects for access to their own personal data and for information as to how and for what purpose(s) it is being processed by Florence.

- **Right to data portability:** Where processing is based upon the lawful basis of consent, or for the performance of a contract with the data subject, Florence process for responding to requests from data subjects will allow individuals to obtain and reuse their personal data for their own purposes across different services.

- **Right to erasure ('right to be forgotten'), right to restriction of processing, and right to object to processing:** Florence will have a process to manage and respond to requests from data subjects that we should erase their personal data. Florence will have a process to manage and respond to requests from data subjects for the restriction of processing of personal data concerning the individual in specified ways or in specific circumstances. Florence will also have a process to manage and respond where a data subject objects to the processing of their personal data by Florence, on grounds relating to the individual personal situation.

  These processes will recognise that these rights are qualified, and may be refused where Florence needs to continue processing the personal data for legitimate reasons (with a lawful basis), including where it is necessary and in the public interest to do so for the exercise of our functions or in relation to legal claims.

- **Right to rectification:** Florence will have a process to manage and respond to requests from data subjects for the rectification of inaccurate personal data concerning the individual.

- **Rights in relation to automated decision making, including profiling:** Florence will not use automated processing, without meaningful human input, to profile individuals or make decisions which significantly affect those data subjects, other than with the explicit consent of the data subject or where the processing is explicitly laid down in law. If Florence proposes to undertake such automated processing, this will be clearly communicated in published privacy notices.

Data protection by design and default, and data protection impact assessment (DPIA).

- Florence will ensure that any new process or change which is likely to result in a high risk to privacy, or to the rights and freedoms of data subjects, is first subject to a DPIA.
- This DPIA will include steps to establish the lawful basis for processing, and to understand and mitigate the likely risks.

The DPIA shall also ensure that the processing of personal data is minimised, and that appropriate technical and organisational measures are integral to the design and operation of systems and processes that involve processing of personal data.

Only transferring personal data outside of the UK or European Economic Area (EEA) where we have adequate assurance that it is lawful to do so and that appropriate protections are in place.

- Where possible and practicable, Florence will process personal data within the UK/EEA. Florence will only process personal data outside of the UK/EEA where we have undertaken a DPIA and are satisfied that the personal data is afforded equivalent levels of protection as it would if processed within the UK/EEA, and that the transfer is lawful.

Notification of Data Breaches

Florence will have a process under our Information Governance policy to ensure that data protection breaches are reported to the Information Commissioner's Office, if applicable and notified to data subjects, as required under data protection law.

Subject Access Requests

Florence's Deputy Data Protection Officer supports the administration of processing requests. DPPO is responsible for registering and acknowledging requests, including the validation of identity and legal status. They will also act as a point contact for requesters, clinicians and managers. They will hold documentation to ensure record keeping to demonstrate that a request has been processed in accordance with the legislation e.g. keeping an accurate record that identity documents have been viewed.

Subject Access Request Process

1. Receiving requests made in writing to gdpr@florence.co.uk;
2. If more than one service/department needs to be involved the DDPO will co- ordinate the registration, documentation and monitoring with support from the DPO.
3. Electronically registering the request and sending an acknowledgement in writing;
4. Locating the record and arranging for it to be retrieved understanding the requirements of the request e.g. completing a Subject Access Request form and seeking clarity from the requester if it is not clear notifying the user request or line manager (staff request) that a SAR needs to be dealt with;
5. Validate identity, legal status e.g. power of attorney;
6. Identify information to be redacted and briefly document, on the user/staff record and on the SAR central system, what has been redacted and why;
7. Photocopying the record once the user/staff has identified, extracted and redacted the information seeking advice from the DPO
8. Sending the approved final response in writing;
9. Maintaining the Subject Access Request register and monitoring progress, including ensuring that records are accurate and up to date;
10. Obtaining formal sign-off from user/staff that the information to be disclosed is correct;
11. Closing the request.

Consent

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the Data Protection Legislation, which include Consent. A Data Subject Consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are

insufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects can easily withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first Consented.

When processing Special Category Data or Criminal Convictions Data, we will usually rely on a legal basis for processing other than Explicit Consent or Consent if possible. Special Category Data may be particularly relevant when collecting personal data and work information from a candidate or temporary worker, therefore, we take particular care whenever collecting and processing such information and follow the Company processes when processing this Special Category Data.

Transparency (Notifying Data Subjects)

The Data Protection Legislation requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information is provided through appropriate Privacy Notices which are concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we provide the Data Subject with all the information required by the Data Protection Legislation including how and why we will use, Process, disclose, protect and retain that Personal Data through a Privacy Notice which is presented when the Data Subject first provides the Personal Data to the Company. We review our Privacy Notice regularly and ensure we understand how and why we use Data Subjects Personal Data.

When Personal Data is collected indirectly (for example, from a third party or publicly available source), we provide the Data Subject with all the information required by the Data Protection Legislation as soon as possible after

collecting/receiving the data. We also check that the Personal Data was collected by the third party in accordance with the Data Protection Legislation and on a basis which contemplates our proposed Processing of that Personal Data.

We always comply with the Company's Privacy Notice at all times when collecting data. A copy of the privacy notice can be found here.

Data Minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed. We will only Process Personal Data when it is required to perform our job duties and services. We will not Process Personal Data for any reason unrelated to job duties, or collect excessive data. Any Personal Data collected is adequate and relevant for the intended purposes.

We ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with our data retention guidelines.

Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when found to be inaccurate.

We will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. We check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. We also take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We do not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

We will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held unless a law requires such data to be kept for a minimum time.

Staff are required to take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with all the Company's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

We ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Data Retention and Disposal

We will retain Personal Data for a reasonable duration to provide a Candidate or care professional with our services, or support our Company Personnel, as follows:

Organisation	**Category**	**Purpose/Activity**	**Type of data**	**Legal basis**
Flex, Academy	Clients	**To register you or your employer as a Client**	a. Identity Data b. Contact Data	Necessary for performance of a contract with you
Flex (only)	Clients	**To provide you with our services** including: ● operating the Platform; ● allowing you to communicate with other Members;	a. Identity Data b. Contact Data c. Financial Data d. Community Data	Necessary for: i. performance of a contract with you; ii. our legitimate interests to operate the

		• allowing you to post Vacancies and find WORKERs to fill those Vacancies; • managing payments, fees and charges including via Payment Processor(s); and • collecting and seeking to recover money owed to us.		Platform and those of other Members; and iii. necessary for our legitimate interests (to recover debts due to us).
Flex (only)	Workers	**To register you as a Worker** including making enquiries of third parties, for example, via a Verification Services Provider (see section 5 below).	a. Identity Data b. Contact Data c. Career History and Education Data d. Employment Status Data e. WORKER Profile Data	Necessary for performance of a contract with you
Flex (only)	Workers	**To provide you with our services** including: • operating the Platform; • allowing you to amend your profile; • allowing you to communicate and interact with other Members; • allowing you to apply for Vacancies, accept invitations from Clients and enter into Assignments with Clients; • managing payments, fees and charges including via the Payment Processor; and	a. Identity Data b. Contact Data c. Financial Data d. Services Data e. Career History and Education Data f. Employment Status Data g. WORKER Profile Data h. Community Data	Necessary for: i. performance of a contract with you; ii. our legitimate interests to operate the Platform and those of other Members; and iii. our legitimate interests (to recover debts due to us).

		• collecting and seeking to recover money owed to us.		
Flex (only)	Workers	**For compliance** purposes – Clients (as healthcare institutions) will need to access the personal data of an WORKER via the Platform in order: • to assess the WORKER against the compliance standards set by the Client organisation ahead of arrangement of an Assignment; and • to maintain records of WORKERs with whom the Client has entered into Assignments.	a. Identity Data b. Contact Data c. Profile Data d. Referee Data	Necessary for: i. performance of a contract with you; ii. our legitimate interests to operate the Platform and those of other Members.
Flex (only)	Clients and Workers	**To communicate with relevant regulatory bodies** including the Nursing and Midwifery Council and/or the Care Quality Commission.	a. Identity Data b. Contact Data c. Worker Profile Data d. Services Data	Necessary for: i. performance of a contract with you; ii. to comply with a legal obligation; iii. for our legitimate interests and those of any applicable regulators.
Flex, Academy	Members, Clients and Workers	**To manage our relationship with you** which will include: • notifying you about changes to our Terms and	a. Identity Data b. Contact Data c. Marketing and	Necessary for: i. performance of a contract with you;

		Conditions or Privacy Notice; and • asking you to leave a review or provide feedback.	Communications Data d. Services Data	ii. to comply with a legal obligation; iii. our legitimate interests in keeping our records updated and studying how Members use our Platform and services.
Flex (only)	Applicants	**To consider you for a role,** if you are applying for a job with us	a. Identity Data b. Contact Data c. Career History and Education Data d. Employment Status Data e. Financial Data	Necessary: i. To take steps in order to enter a contract with you; ii. for our legitimate interests in finding employees; iii. to comply with our legal obligations, such as to make reasonable adjustments.
Flex (only)	Referees	**To perform our services** to Workers and Clients and to enable us to obtain your opinions on an Applicant.	a. Identity Data b. Contact Data	Necessary for our legitimate interest in providing our services to Clients and WORKERs, and obtaining information about Applicants

Flex, Academy	Suppliers	**To carry out our contractual obligations** to you, if you are our supplier or subcontractor, including to manage our payments to you.	a. Identity Data b. Contact Data c. Financial Data d. Services Data	Necessary for our legitimate interests in receiving services from our suppliers to ensure our business is run efficiently.
Flex, Academy	Members and Platform Visitors	**For security purposes and to administer our Platform** – to maintain and enhance the Platform, to ensure that content from it is presented in the most effective manner for you and your computer, and to enhance the user experience (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).	Technical Data	Necessary: i. for our legitimate interests in running our business, to ensure the security of our systems, to assist us in the provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or company restructuring exercise; ii. for performance of a contract with you; iii. to comply with a legal obligation.
Flex, Academy	Members, Clients	**To provide you with marketing information** relating to the	a. Identity Data b. Contact Data	Necessary for our legitimate interests to

	and Workers	services and activities which you request from us or which we feel may be of interest to you, and relevant Platform content, and to measure or understand the effectiveness of the marketing we serve to you.	c. Services Data d. Marketing and Communications Data e. Technical Data	develop our services, grow our business and inform our marketing strategy.
Flex, Academy	All categories	**Business and analysis purposes** - for business monitoring, assessment and analysis of our Clients, Workers and Members, to develop our business strategy, record keeping including maintaining our accounts, complying with good practice and for other administrative, operational and security reasons, and to seek your thoughts and opinions on the services we provide.	a. Identity Data b. Contact Data c. Services Data d. Marketing and Communications Data e. Technical Data	Necessary: i. for our legitimate interests in running our business efficiently, successfully and in order to keep our records updated; ii. to comply with a legal obligation.
Flex, Academy	Members and Platform Visitors	**To improve the Platform and the services**, services, customer relationships and experiences.	a. Technical Data b. Services Data	Necessary for our legitimate interests in understanding how Members use our services, keeping the Platform updated, and developing our business and to inform our marketing strategy.
Flex (only)	Members, Workers, Clients and Referees	**As required in special circumstances such as a police or other legal investigation** or serious complaint requiring a Client, a	a. Identity Data b. Contact Data c. Worker Profile Data	Necessary for: i. performance of a contract with you;

		Worker and/or Florence to release personal data.	d. Employment Status Data e. Career History and Education Data f. Services Data g. Marketing and Communications Data h. Technical Data i. Special Categories of Data	ii. compliance with a legal obligation; iii. performance of a task in the public interest;. iv. the establishment, exercise or defence of legal claims or whenever courts are acting in tier judicial capacity;
Flex (only)	Workers	**As required in limited circumstances, when a Client must use personal data to help it discharge its functions relating to providing care to patients** and relatives and looking after their welfare.	a. Identity Data b. Contact Data c. Worker Profile Data d. Services Data e. Technical Data f. Marketing and Communications Data	Necessary for: i. Performance of a contract with you; ii. Compliance with a legal obligation; iii. Public interest.
Flex, Academy	All categories	**To prevent and detect crime, fraud or corruption** and to meet our legal, regulatory and ethical responsibilities	a. Identity Data b. Contact Data c. Technical Data d. Services Data	Necessary to comply with our legal obligations

For many types of HR records, there is no definitive retention period and we are required to consider carefully how long to keep them. We have based our records

retention periods on the time limits for potential UK tribunal or civil claims and guidance in the Conduct of Employment Agencies and Employment Businesses Regulations 2003. The UK Limitation Act 1980 contains a 6-year time limit for starting many legal proceedings, so where documents may be relevant to a contractual claim, we will keep these records for at least this period. Other records may be retained longer or permanently. These retention periods are in line with CIPD recommendations.

Disposal of Records

Electronic records will be securely and permanently deleted as appropriate and Florence has facilities for the secure disposal of documentation relating to Care Professionals, employees and clients. The destruction of any electronic data is co-ordinated with the Tech Team and conducted in a safe and organised manner which puts the Personal Data beyond recovery. The method of destruction is appropriate to the sensitivity or security classification of the information. Paper records are disposed of in confidential waste.

We will maintain records of disposal and will detail the date and the name of the person who authorised the record's disposal for all records that are either deleted or destroyed.

Under current data protection laws, Data Subjects (in this care professionals) have a right to request that we delete their Personal Data. However, this is not an absolute right - where we have another legal basis to continue to process that data, (e.g. we have a legal obligation to hold certain records for a certain period of time), those obligations will take precedence over the Data Subject's right.

Confidentiality

Our staff are provided with instructions relating to confidentiality during induction, as part of their contract and in the staff handbook. This instructs them to:

- Ensure confidential information is stored securely.
- No disclose confidential information without explicit written Consent from the disclosing party.

- Notify the disclosing party if unauthorised access, copying or use of the information is suspected.

Confidential information is disclosed to our staff on a "need to know" basis to enable us to meet our obligations under our contractual frameworks.

Training

Data Security and Protection training is mandatory and all staff are required to complete annual on-line Information Governance training. All Florence staff are required to read the Employee Handbook and accept the declaration

Training on core IT Security related topics include:

- Password Strength/Security
- Two Factor Authentication
- Phishing attack awareness
- Smishing / Vishing attacks
- Penetration testing
- Responsibilities for equipment
- Reporting Responsibilities
- Data Privacy
- An understanding of all relevant Information Security Policies

Disaster Recovery, Contingency and Business Continuity

Florence approaches protecting our own devices in a secure way. Florence will provide training and support to enable all employees to do so (see below). Any violation may result in disciplinary measures.

At a minimum:

- Remove software that do not use or need from any computer
- Update operating systems and applications regularly and when prompted
- Keep the computer firewall and antivirus switched on
- Store files in official company storage locations so that it is backed up properly and available in an emergency

- Switch on whole disk encryption
- Understand the privacy and security settings on work phones and social media accounts
- Do not share company devices with anyone else
- An Administrator account exists on every laptop for IT Administrators to perform updates/administrative tasks. Access to this administrator account is prohibited.
- A local user account is provided for employee use. This must be the only account used on any employee account.
- Make sure computers and phones log out automatically after a max of 15 minutes and require a password to log back in.

Reporting information losses

All staff of Florence have a duty to report the loss, suspected loss or unauthorised disclosure of any Florence's information asset to the DPO and Head of Technology and Security.

Reporting information security breaches

All staff of Florence have a duty to report breaches, suspected breaches of any Florence's information asset to the DPO and Head of Technology and Security. Breaches of the Information Security Policy may be treated as a disciplinary matter dealt with under Florence's staff disciplinary policies.

Incident management and escalation

All staff are responsible for reporting Information Governance incidents.

Managers must notify Florence's Data Protection Officer of any Incidents by email to gdpr@florence.co.uk.. There is no simple definition of an incident. Incident requiring investigations are incidents which involve actual or potential failure to meet the requirements of the Data Protection Legislation and /or the Common Law Duty of Confidentiality. This includes unlawful disclosure or misuse or confidential data, recording or sharing of inaccurate data, information security breaches and inappropriate invasion of people's privacy.

The Data Protection Officer will report a notification to the Information Commissioner's Officer (ICO)

The Data Protection Officer will work with the relevant service/department managers to ensure that incidents are appropriately investigated and that the required documentation is completed and provided to the Information Commissioner's (ICO) as required.

Backup and disaster recovery

Information owners must ensure that tested backup and system recovery procedures are in place. Backup of Florence's information assets and the ability to recover them are important priorities. All system managers must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of datafiles; especially where such files may replace files that are more recent.

Mobile and Remote Computing

Authorisation

Those remotely accessing information systems, data or services containing sensitive or confidential information must be authorised to do so by an appropriate authority, usually the line manager.

Travelling

Portable computing or storage devices are vulnerable to theft, loss or unauthorised access when travelling. All Florence approved mobile and laptop device management software must be installed and activated at all times. The device management is managed by a third party organisation, Employee Xero. Devices must be provided with an appropriate form of access protection such as a password or encryption to prevent unauthorised access to their contents. In addition, more recent means of authentication such as Touch-ID or Face-ID are also acceptable forms of access protection.

Equipment and media should not be left unattended in public areas and portable devices should be carried as hand luggage. To reduce the risk of unauthorised access, automatic shutdown features have been introduced to

all devices installed by Employee Xero. Passwords or other similar security measures for access to Florence's systems should never be stored on mobile devices or in their carrying case. Screens on which sensitive or confidential information is processed or viewed are fitted with a privacy filter or be sited in such a way that they cannot be viewed by unauthorised persons.

Outsourcing and Working With Third Parties

Third Party: An organisation or person, who supplies goods, services and / or consultancy to Florence and who will or are likely to have access to Personal Confidential Data as part of Florence's information assets. Information assets may be accessed within Florence's premises or external to Florence premises.

Florence must:

Ensure that where a Third Party is to be engaged, an appropriate Data Protection Impact Assessment (DPIA) in accordance with Florence DPIA Framework Guidance is carried where appropriate to identify the scope of any information required for the purpose of the contract and the legal basis for sharing the information. The DPIA template is included within the DPIA Framework Guidance (which can be found on Florence intranet) or can be obtained from the Governance Team.

Ensure that, where required (as identified from the DPIA) that a Data Sharing Agreement (DSA) is also completed.

Ensure that the transfer of any data is risk assessed, justified and not excessive for the purpose of the data required / requested.

Ensure copies of the signed agreement are held by both the Third Party and the Information Asset Owner (IAO).for services.

Ensure that any confidential information communicated to the Third Party is completed securely and in accordance with Florence policy.

Report immediately, any suspected or actual information security breaches / personal data breaches involving the third party through Florence incident reporting process (please refer to the Incident and Complaints Policy)

Third Parties must:

Treat all information received from Florence as confidential; which may be derived from or be obtained in the course of any contract, agreement or any other arrangement between Florence and those third parties; or which may come into the possession of the Third Party or an employee, servant, agent or sub-contractor of the Third Party as a result or in connection with the contract; and

Provide all necessary precautions to ensure that all such information is treated as confidential by the Third Party,

Ensure that all employees, users, agents and subcontractors are aware of the provisions of the DPA 2018 and General Data Protection Regulations.

Ensure that they are registered accordingly under the DPA and that any personal information obtained from Florence shall not be disclosed or used in any unlawful manner; and

Indemnify Florence against any loss arising under the DPA caused by himself, his employees, servants, agents or subcontractors.

Use of Cookies & Similar Technologies

A cookie is a small text file that is downloaded onto 'terminal equipment' (e.g. a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

The information we may collect in this manner includes IP address, unique device identifier, browser characteristics, device characteristics, operating system, language preferences, referring URLs, information on actions taken on our website(s), dates and times of visits to our website(s) and other usage statistics.

In line with regulation 6 of the PECR, when people visit our website, we:

- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person's Consent to store a cookie on their device.

We then allow them to set their preferences to accept or reject cookies by obtaining Explicit Consent. Restricting or rejecting cookies on our website may, however, mean that certain areas of the site will not function correctly.

We may also use third-party apps, tools, plug-ins and widgets on our website(s), and these may use automated means to collect information relating to how you interact with these features. Such information collected is subject to the privacy policies of those providers and to applicable law. Florence is not responsible for the practices of these providers.

These are the cookies we use and why:

Cookie Title	**Cookie Name**	**Category**	**Purpose**	**Duration of Cookie**
Florence	__florence_session	Strictly necessary	This cookie is used to identify a user's session and temporarily store a unique identifier for that session. It is essential for the functionality of forms on our website.	30 days
Google Universal Analytics	_ga _gali _gat_UA-1036645-1 _gid	Analytical / performance	These cookies are used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website and blog, where visitors have come to the website from and the pages they visited. Read Google's overview of privacy and safeguarding data here.	10 years
Cloudflare	__cfduid	Security	The *__cfduid* cookie is used to identify individual clients behind a shared IP address and apply security settings on a per-client basis. For example, if a visitor is in a coffee shop where there may be several infected	1 year

			machines, but the specific visitor's machine is trusted (for example, because they completed a challenge within your Challenge Passage period), the cookie allows Cloudflare to identify that client and not challenge them again. It does not correspond to any user ID in your web application, and does not store any personally identifiable information.	
Drip	_drip_client_{HASH}	Analytics	This cookie allows us to identify logged in users for our email platform.	2 years
Facebook	_fbp	Analytics	These cookies are used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. The cookies collect information in an anonymous form, including the number of visitors to the website and blog, where visitors have come to the website from and the pages they visited. For more information visit: https://www.facebook.com/legal/technology_terms	1 day
Sumo	__smToken	Targeting	The **__smToken** is set once you login to Sumo and is checked to verify whether you are logged into Sumo or not.	6 months
Intercom	intercom-id-{HASH} intercom-lou-{HASH}	Functionality	This cookie is used by Intercom to recognise if you have visited the website before, and to list your past conversations.	6 months

Median	mdn_anonymous_id	Analytical/ performance	This cookie allows you to share your screen with us, so we can help you with troubleshooting.	10 years
ShareThis	attrb attru attrg	Analytics/performance	These cookies are used by Share This to track the sharing of content	1 year
Full Story	fs_uid	Analytical/ performance	These cookies identify the visitor in a third-party service we use for replaying sessions from users. We use these cookies to help us understand how users interact with our site and to replicate any issues users may encounter.	Persistent
Trustpilot	amplitude_id_*	Analytical/ performance	Used by Trustpilot and Segement for analytics.	10 years
Optimizely	optimizelyBuckets optimizelyEndUserId optimizelySegments	Analytical/ performance	Optimizely is one of our chosen A/B testing solutions. The service is provided by Optimizely, Inc.. The cookies hold short alphanumeric string values to store page variant and experiment data. The cookies do not store any personally identifiable information. The first three of these cookies may be set as Third Party cookies if your session spans multiple top-level domains.	9 years
Segment	ajs_anonymous_id ajs_group_id ajs%3Acookies ajs%3Atest ajs_user_id	Analytical/ performance	Segment IO cookies to identify known users and track their site activity	1 year

Access by Data Subjects

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

The Right to be Informed

We aim to be transparent within our privacy policy and provide information about how we use personal data.

The Right to Object

In some circumstances individuals can stop the processing of their personal information for reasons connected to their individual situation. We then do so unless we believe we have a legitimate overriding reason to continue processing their personal data.

Where personal details are used for marketing, individuals can opt out at any time. They are able to unsubscribe from marketing on each contact or can contact us to object to any processing.

The Right to Rectification

Everybody has the right to request the correction of their personal information when it is incorrect, out of date or incomplete. If we are notified that personal information we hold is complete or inaccurate we will correct or complete the information as soon as possible.

The Right to Erasure or the Right to be Forgotten

Everyone has the right to request that their personal information is deleted; including if we no longer need it for the purpose we collected it, the person withdraws their consent or objects to its processing.

Following a request, we will erase the personal data without undue delay unless continued retention is necessary and permitted by law. If we make the personal

data public, we shall take reasonable steps to inform other data controllers processing about the individual's erasure request.

The Right to Restrict Processing

Everyone has the right to request that we restrict the processing of their personal information. This can be done in circumstances where we need to verify the accuracy of the information, if the person does not wish to have the information erased or has objected to the processing of the information, and we are considering this request. Once the processing is restricted, we will only continue to process the personal data with consent, or if we have another legal basis for doing so.

The Right to Access

Individuals have the right to access the personal information we hold about them. Any access request will usually be free of charge and responded to within one month. We will endeavour to provide information in the format requested, but we may charge a reasonable fee for additional copies.

The Right to Data Portability

Everyone has the right to receive a copy of their personal information which has been given to us. The copy will be provided in a commonly used and machine-readable format. We can also transmit it directly from us to another data controller, where technically possible.

We will verify the identity of an individual requesting data under any of the rights listed above and will not allow third parties to persuade us to disclose Personal Data without proper authorisation.

Any Data Subject request must be forwarded to the Deputy Data Protection Officer who will record the date, details and all communication relating to the request. All responses to a Data Subject request will be made in writing and the Deputy Data Protection Officer will respond to requests within 30 days unless the request is complex in which case it may take longer.

Whilst a Data Subject may ask us to delete their data, we must comply with a wide range of legislation and regulation including but not limited to HMRC, RIDDOR, the Working Time Regulations, the Agency Workers Regulations, the Nurses Agencies Regulations 2002 and this may mean that we are unable to fulfil such a request. As a minimum we are required to retain copies of:

- Agreements between us and our care professionals.
- Recruitment and selection records for nurses that have been supplied.
- Records of any statement given to a client about the qualifications and experience of our care professionals.
- Client details including contact details for key personnel.
- Details of all care professionals supplied or available for supply.
- Details of all placements.
- Details of each care professionals training records, appraisals and feedback received from the client.
- Details of any allegations of abuse against a care professional including investigations, outcomes and actions taken in consequence.

Right of Audit

Florence operates many contracts where we are obliged to provide access to client and candidate information for quality and audit purposes. Work seekers will be asked to sign a UK GDPR data protection disclaimer on their application form to give us permission to share their Personal Data with clients and any external auditors as required to support audits.

Audits are a method to ensure that Florence is compliant with relevant Information Governance Policies and Procedures. Audits must be completed on a regular basis to enable Florence to demonstrate compliance with the General Data Protection Regulations.

The objectives are as follows:

- To ensure that Information Governance Policies and Procedures are adhered to within Florence
- To provide assurance in relation to data protection compliance across the organisation

- Record information accurately and reliably
- Use information effectively and ethically
- Protect information against unauthorised access
- Ensure regulatory and legislative requirements are met

Implementation

The Data Protection Officer will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Data Protection Officer who will have overall responsibility for:

- The provision of cascade data protection training, for staff within the company.
- For the development of best practice guidelines.
- Carrying out compliance checks to ensure adherence with the General Data Protection Regulations.

Record Creation & Management by Temporary Nurses Working at Participating Authorities

Care Professionals will follow the records management procedures in place at the Participating Authority they are working. Regardless of the media on which the records are kept, care professionals must ensure that all records are complete, reliable, authentic and available and in an accessible format. Records must:

- Provide adequate evidence to account for all financial transactions including reasons for any decision(s) necessary for that transaction to take place.
- Contain verifiable evidence that all transactions were appropriately undertaken and where necessary were properly authorised.
- Provide complete information to document the transactions.
- Demonstrate the delivery of care, treatment and services.
- Comply with regulatory and accountability record-keeping requirements.
- Be comprehensive and document the complete activity i.e. contain a full audit trail.

Records are required to accurately reflect communications, decisions and actions taken to:

- Allow employees, nurses and midwives and their successors to undertake appropriate actions in the context of their responsibilities.
- Facilitate an audit or examination by anyone authorised to do so.
- Protect the legal and other rights of the participating authority, its patients, staff and any other people affected by its actions.
- Provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

6. Records Management

This policy supports Florence's records management requirements and includes four key activities. Records Management is the practice of managing the records of an organisation throughout their lifecycle, from creation or receipt to their eventual disposal or transfer to permanent storage.

A Record is information created, received and/or maintained as evidence by Florence in its pursuance of legal obligations or business transactions, regardless of format.

Florence will provide training and guidance to ensure staff understand their legal responsibilities and can apply best practice in managing records. The key benefits for supporting Florence in this are that records are:

- Captured and stored in the right place
- Authentic so Florence are confident that records are accurate
- Accessible in a timely way, by those who need or have a right to see them
- Protected from unauthorised deletion, changes or access
- Disposed of appropriately once they are no longer required

Records should be held in electronic format to meet the requirements of the government's digital strategy and to support easy access. Therefore, the policies and associated guidance that support this policy are designed to achieve this

goal while also supporting management of records that only exist in paper format.

Four Key Activities of Records Management

Planning

Policies and guidance will be planned and updated to provide support for:

- Maintaining an accurate Information Asset Register
- Training all staff
- Changes in legislation or business requirements.

Creating and capture

- Policies and guidance support the identification of records and define standards for:
- Naming electronic records
- Managing paper and handwritten records
- Scanning paper records to ensure they comply with current legal requirements and best practice when creating electronic records
- Managing emails which are Florence records.

Storage, maintenance and access

Policies and guidance support record storage and maintenance by defining standards for:

- Protecting sensitive or confidential information
- Sharing records
- Version control
- Storing and maintaining paper
- Managing records within shared systems, including emerging technologies such as the Cloud.

Retention, review and disposal

Policies and guidance define the processes and methods for managing records at the end of their lifecycle by defining standards for:

- Identifying retention periods for categories of records based on business need and legislative requirements
- Supporting the secure disposal of records
- Defining which records need preserving and the procedures associated with this.

7. Monitoring and Compliance

This policy will be reviewed regularly and may be altered from time to time in light of legislative changes or other prevailing circumstances.

8. References and Further Guidance

- Data Protection Act 2018
- General Data Protection Regulation (Regulation (EU) 2016/679)
- Freedom of Information Act 2000
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended)
- Environmental Information Regulations 2004
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) Regulations 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Malicious Communications Act 1988
- Digital Economy Act 2010
- Intellectual Property Act 2014
- Investigatory Powers Act 2016

9. Policy Changes/Version History

Date	Reviewed changes