INFORMATION GOVERNANCE POLICY

1. QUICK REFERENCE GUIDE

1.1 This overarching policy provides guidance and lays the framework for Information Governance at the Forest Skin Clinic (the “FSC”).
1.2 FSC hold all their clinics within an NHS building and as such are required to follow the local guidance. This policy will highlight areas specific to FSC that are on top of local policy.

2. INTRODUCTION

2.1 The policy is intended to be fully consistent and compatible with the policies and practices adopted by the FSC.
2.2 It has been developed to achieve compliance to the Care Quality Commission (CQC) Outcomes.
2.3 The Forest Skin Clinic is committed to treating people with dignity and respect in accordance with the Equality Act 2010 and Human rights Act 1998. Throughout the production of this guideline due regard has been given to the elimination of unlawful discrimination, harassment and victimisation (as cited in the Equality Act 2010).

3. PURPOSE

The purpose of this policy is to provide details of the framework for implementation of the Information Governance strategy to enable FSC to meet its Privacy and Data Protection Legislation obligations including any statutory Information Governance and Data Security responsibilities.

4. BACKGROUND

4.1 Underpinned by the core values where we will make sure that patients get the very best quality health care by providing individualised, evidence-based, holistic care in a mutually respectful partnership. Our mission is to ensure that proper data management and proper technical measures exist and are embedded throughout the FSC.
4.2 Information is a valuable resource. Its loss can damage reputations and services, its misuse can damage organisations and individuals. It plays a key part in clinical governance, service planning and performance management.

4.3 It is of paramount importance to ensure that information is effectively and efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management and security.

5. SCOPE

5.1 This policy applies to all staff handling information at the FSC including registered practitioner, administration staff and contractors.

5.2 This policy also applies to;

- All information held and processed by the FSC;
- All information systems managed by the FSC;
- Any individual using information owned by the FSC;
- Any individual requiring access to information owned by the FSC.

6. RESPONSIBILITIES

6.1 All staff are responsible for ensuring that they:

6.1.1 Are familiar with the GDPR principles, Caldicott Guardian principles and other documented procedures and policies including acceptable e-mail use and information security, all policies are available via the intranet site of the NHS working site and can be accessed by the Clinical Director for dissemination.

6.1.2 Carry out their day to day work in accordance with best practice confidentiality and data protection procedures and legislation.

6.1.3 Keep up to date with best practice confidentiality and data protection procedures and legislation through undertaking annual Information Governance training.

6.2 The FSC Directors undertake the following roles:

- **Accounting Officer** - overall responsibility for Information Governance and Data Security at the Trust. This individual is ultimately responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Maintaining confidentiality is pivotal to being able to supply a first-class confidential service that provides the highest quality patient care.

- **Caldicott Guardian** - responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. Ensuring that the FSC satisfies the highest practicable standards for handling patient identifiable information and will bring clinical Information Governance issues to the attention of the IGSG as appropriate.

- **Senior Information Risk Owner** - familiar with and takes ownership of the organisation’s Information Risk policy, acts as advocate for Information Risk
and accountable for the corporate responsibility for the Information Governance framework, strategy, policies including Data Quality and Records Management.

- **Data Protection Officer** - a legal role required by the GDPR. Responsible for overseeing the Information Governance strategy and the implementation of data protection and security measures to ensure compliance with the GDPR requirements, these measures should ultimately minimise the risk of breaches and uphold the protection of personal identifiable and special categories of data.

7. **PRINCIPLES**

7.1 The FSC is committed to ensuring that the Caldicott Guardian principles and GDPR principles exist as the heart of all personal data processing, acknowledging the need for Lawfulness, fairness and transparency; Purpose limitation; Data minimisation; Accuracy; Storage limitation; Integrity and confidentiality (security) and Accountability.

7.2 The FSC recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

7.3 The FSC also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

7.4 The FSC believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all staff to ensure and promote the quality of information and to actively use information in decision making processes.

7.5 The FSC’s Information Governance objectives are to:

- Hold information securely and confidentially;
- Obtain information fairly and efficiently;
- Record information accurately and reliably;
- Use information effectively and ethically;
- Share information appropriately and lawfully.

8. **DATA SECURITY AND PROTECTION TOOLKIT REQUIREMENTS**

8.1 The FSC is committed to meeting its statutory Data Security and Protection requirements, including implementing and overseeing the Data Security and Protection (DSP) Toolkit, also the ten data security standards from the Office for the National Data Guardian.

8.2 The ten data security standards are as follows:

<table>
<thead>
<tr>
<th>LEADERSHIP OBLIGATION 1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>People:</strong> Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles</td>
</tr>
<tr>
<td>Data Security Standard 1</td>
</tr>
<tr>
<td>-------------------------</td>
</tr>
<tr>
<td>Data Security Standard 2</td>
</tr>
<tr>
<td>Data Security Standard 3</td>
</tr>
<tr>
<td>LEADERSHIP OBLIGATION 2</td>
</tr>
<tr>
<td>Data Security Standard 4</td>
</tr>
<tr>
<td>Data Security Standard 5</td>
</tr>
<tr>
<td>Data Security Standard 6</td>
</tr>
<tr>
<td>Data Security Standard 7</td>
</tr>
<tr>
<td>LEADERSHIP OBLIGATION 3</td>
</tr>
<tr>
<td>Data Security Standard 8</td>
</tr>
<tr>
<td>Data Security Standard 9</td>
</tr>
<tr>
<td>Data Security Standard 10</td>
</tr>
</tbody>
</table>
9. RESPONSIBILITIES OF THE FSC

9.1 All information used in the FSC is subject to handling by individuals and it is necessary for these individuals to be clear about their responsibilities.

9.2 The FSC must ensure legal requirements are met, including investigating and reporting Information Governance incidents which meet the specified threshold.

10. LEGAL AND REGULATORY FRAMEWORK

10.1 There are a number of legal obligations placed upon the FSC for the use and security of personal data and special categories of data.

10.2 There are requirements to appropriately disclose information when required.

10.3 There are Codes of Practice and operating procedures adopted by the FSC.

10.4 The adopted policy contains further details of the legal and regulatory framework.

10.5 The FSC only operated under agreed Insurance Terms and Conditions.

11. KEY ELEMENTS OF THE INFORMATION GOVERNANCE FRAMEWORK

11.1 Freedom of Information:
   11.1.1 Non-confidential information about the FSC and its services will be available to the public through a variety of media;
   11.1.2 Patients have ready access to information relating to their own health care, their options for treatment and their rights as patients;

11.2 GDPR Compliance:
   11.2.1 The FSC will ensure that the GDPR principles exist as the heart of all personal data processing.
   11.2.2 The FSC will maintain its Privacy Notice to inform individuals what to expect about the use of personal information, what we may collect and hold about, our purposes including whom we may share it with, how we look after it, individuals rights and where individuals can obtain further information.

11.3 Legal Compliance:
   11.3.1 The FSC regards all identifiable personal data relating to patients as confidential;
   11.3.2 The FSC regards all identifiable personal data relating to staff as confidential except where national policy on accountability and openness requires otherwise;
   11.3.3 The FSC will maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act);

11.4 Information Security
   11.4.1 The FSC will maintain standards and policies for the disclosure of information;

11.5 Information Quality Assurance:
11.5.1 Registered Practitioners are expected to take ownership of, and seek to improve, the quality of information within their services;
11.5.2 Wherever possible, information quality should be assured at the point of collection;

11.6 Records Management:
11.6.1 The FSC uses Pabau.com Electronic Patient Records System for all patient related documentation.
11.6.2 The FSC maintain policies and procedures for the effective management of records via Pabau.

11.7 Information Governance Training:
11.7.1 All FSC staff will undergo external Information Governance Training on an annual basis and produce evidence of training to the Directors.

11.8 Management of Information Governance
11.8.1 The FSC Directors are responsible for implementing Information Governance policy.

12. COMPLIANCE WITH THIS POLICY

The accountability code within Article 5(2) to the GDPR requires the FSC demonstrate compliance with the principles. Therefore, the FSC has a legal obligation to implement technical, security and organisational measures to demonstrate that data protection has been integrated to processing activities by design and by default.

13. INCIDENTS REQUIRING INVESTIGATION
13.1 It is essential that all Information Governance Incidents Requiring Investigation which occur at the FSC are reported appropriately and handled effectively.
13.2 All staff are responsible for reporting information incidents such as information being illegitimately accessed, used, disclosed, altered, destroyed, and or stolen, resulting in impairment or loss as soon as possible directly to the FSC Directors (no later than 24 hours after becoming aware of the incident).

14. LEGAL CONSIDERATIONS
14.1 The FSC regards all identifiable personal information relating to patients as confidential and will comply with legal requirements. The FSC regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
14.2 The FSC will ensure compliance the Common Law Duty of Confidence.
14.3 Failure to comply with the data protection regulations could result in reputational damage to the FSC and may carry financial penalties imposed by the Information Commissioner, or other regulatory action.
14.4 Under the GDPR, there are two tiers of administrative fine that can be imposed:
14.4.1 The maximum fine for the first tier is €10,000,000 or in the case of an undertaking up to 2% of total annual global turnover (not profit) of the preceding financial year, whichever is greater.
14.4.2 The second tier maximum is €20,000,000 or in the case of an undertaking up to 4% of total annual global turnover (not profit) for the preceding financial year whichever is greater.

14.4.3 The fines within each tier relate to specific articles within the Regulation that the organisation has breached.

14.4.4 As a general rule, organisations who fail to comply with GDPR principles will result in a fine within tier one, while data breaches of an individual’s privacy, rights and freedoms will result in a fine within tier two.

14.4.5 Failure to evidence that data protection has been integrated to processing activities by design and by default for example ensuring a protection and Privacy Impact Assessment has been carried out may result in a tier one fine.

14.5 Where the law is unclear, a standard may be set, as a matter of policy, which clearly satisfies the legal requirement and may exceed some interpretations of the law.

15. TRAINING

15.1 The Data Security Awareness Level one course is mandated for everyone working in health and care. It has been designed to inform, educate and upskill staff in data protection, data security and information sharing. It provides an understanding of the principles and importance of data security and information governance. It looks at staff responsibilities when sharing information and includes a section on how to take action to reduce the risk of breaches and incidents.

16. REFERENCES

ACKNOWLEDGEMENT: The Princess Alexandra Hospitals NHS Trust for the re-use of core content.
APPENDIX 1

CALDICOTT PRINCIPLES

Further guidance on the Caldicott principles should be obtained from the Department of Health (www.gov.uk) and/or from Information Governance, the seven principles identified in the Caldicott principles are:

1. **Justify the purpose(s):** Every single proposed use or transfer of patient identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use patient identifiable information unless it is necessary:** Patient identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary patient-identifiable information:** Where use of patient identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

4. **Access to patient identifiable information should be on a strict need-to-know basis:** Only those individuals who need access to patient identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

5. **Everyone with access to patient identifiable information should be aware of their responsibilities:** Action should be taken to ensure that those handling patient identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Understand and comply with the law:** Every use of patient identifiable information must be lawful. Someone in each organisation handling patient information 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 patient confidentiality:** Professionals should in the patient's interest share information within this framework. Official policies should support them doing so.
APPENDIX 2

GDPR PRINCIPLES

Further guidance on the GDPR principles should be obtained from the Information Commissioners Office (https://ico.org.uk) and/or from Information Governance, the seven principles identified in the GDPR principles are:

1. **Lawfulness, fairness and transparency**: Personal data shall be, processed lawfully, fairly and in a transparent manner in relation to the data subject.

2. **Purpose limitation**: Personal data shall be, collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.

3. **Data minimisation**: Personal data shall be, adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. **Accuracy**: Personal data shall be, accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5. **Storage limitation**: Personal data shall be, kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.

6. **Integrity and confidentiality (security)**: Personal data shall be, processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

7. **Accountability**: The controller shall be responsible for, and be able to demonstrate compliance.