|  |  |
| --- | --- |
| **SRFT Systems Access Code of Conduct Form**  \*To be Completed by the Trust Sponsor\* | **SRFT-Logo-Full_colour_[web500]** |
| **Classification:** Code of Conduct  **Lead Trust Sponsor:**  (Name/Title/Department/Role)  **Sponsor’s Service:**  **Contact details:** |
| **Scope:** Active Directory (Domain Logon)  **Applicant:**  (Name/Title/Department/Role)  **Applicants Role:**  (eg Locum/Agency/Contract Staff/Student/Research representative)  **Applicants Employer:**  **Contact No.**. | |
| **Associated Documents:**   * All associated documents must be listed. Include Unique ID for Trust documents if known. (specific Data Sharing Agreement/Trust policies) | |
| **Unique Identifier: CofC:**  **Issue number:**  **Authorisation date:**  **Start date:**  **End Date:** | |
| **Purpose of Document:**  This section briefly describes the key purpose of the Code of Conduct.  Relevant details could include reference to guidelines from national organisations/ societies, patient safety incidents, recommendations from the Dept. of Health or HM Coroner or findings from local audit.  To clarify the scope of the Code of Conduct. ‘Scope’ could refer to:   * The Type of Access being given (read only, read/write access) * Audit controls in place to monitor appropriate access * The legitimate legal purpose for allowing access to the Trust system(s) | |
| **Endorsement**  Once the Code of Conduct has been endorsed by with the SIRO/Head of Information Assurance the document should be sent to the appropriate Trust Sponsor to obtain signatures from the applicant  Endorsed by:  Name  Position of Endorser  Date | |

**CODE OF CONDUCT FOR PERSON(S)**

**(Including Locum, Agency & Contract Staff):**

**DATA PROTECTION AND CONFIDENTIALITY**

**All persons accessing Trust systems are required to read this Code of Conduct and signify their agreement to comply with the Code by signing and returning a copy of it to [the Sponsor (names above) / Information Governance Department].**

1. All persons accessing Trust Systems are obliged to comply with any legal requirements in respect of their use of Trust information, be that personal data within the meaning of the Data Protection Act 1998, information belonging to the Trust or otherwise. This includes any requirements pursuant to the Data Protection Act 1998, Access to Health Records Act 1990, common law duty of confidence and, as the Trust is a public body, the Freedom of Information Act 2000.

Furthermore, use of information must be in accordance with relevant professional codes of practice by which persons accessing Trust Systems are bound and any legal requirements relating to intellectual property rights, such as the use of copyrighted material pursuant to the Copyright Designs and Patents Act 1998

In particular: -

1. You agree to comply with the Trust’s Information Governance policies (and/or Terms of a Data Sharing Agreement or contract under which this access is given) copies of which may be obtained from the Trust’s Intranet homepage
   * <http://intranet.srht.nhs.uk/policies-resources/trust-documents/trust-wide-general/imt/>
2. You also agree that, except in the proper course of your duties, as authorised or required by law or as authorised by your line manager, the line manager of the service(s) you are working for or the Trust sponsor, either during your appointment / period of access to the Trust or at any time after that appointment / access, you will not:
   * Process or use any confidential information (including, but not limited to, information in any form relating to conduct of the Trust’s business, information relating to others including personal data of patients, other employees or agents of the Trust and any information marked or described as sensitive personal or confidential or which could reasonably be expected to be confidential);
   * Make or use any copies of personal, sensitive personal or confidential information (including in written, oral, visual or electronic form); or
   * Disclose any such personal, sensitive personal or confidential information to any person, company or other organisation.
3. You shall also use your best endeavours to prevent the use or communication of any such personal, sensitive personal or confidential information by any other person, company or organisation, except in the proper course of their duties, as required by law or as otherwise authorised by the Trust, and shall inform the Information Governance Manager if you become aware or suspect that any such person, company or organisation has used or communicated any personal, sensitive personal or confidential information.
4. In addition: -
   * You shall not attempt to access any restricted areas (areas giving access to information to which you do not have a legitimate working need to access) of the Trust / or Trust systems, unless specifically authorised by your line manager / area manager / Trust Sponsor to do so.
   * You shall not remove from Trust premises, copy, save or otherwise transfer (in writing, orally, visually or electronically) any Trust information (including patient information) except as part of the proper course of your duties or with the prior written permission of your line manager/Trust Sponsor. For the avoidance of doubt, this includes “burning” any information onto a CD, DVD or Blu-Ray disc or copying or saving information to the local drive of a PC or laptop.
   * You shall not give your allocated password to anyone, even another member of staff
   * If you have been issued with or allowed to use a computer, laptop, PDA, telephone or any other device, you shall take reasonable steps to ensure that it is kept secure, never leaving it logged on whilst unattended or in an unlocked area.
   * You shall not download or install any software from external sources without authorisation from the Information Governance Manager
   * You shall not attach any device or equipment to Trust systems [without authorisation and prior screening by the IT department], including but not limited to a MP3 player, iPhone, mobile telephone, PDA or external drive.
   * You shall forward, as soon as possible, any formal written request from a person for access to their personal data (a “Subject Access Request”) to the Information Governance Team. This includes the situation where patients request to see their case notes. Any verbal requests by a person for access to their cases notes or other personal data should also be passed to [the Information Governance team] who will assist that person to make a Subject Access Request.

**Signature \*To be completed by the user\***

I, the undersigned, confirm that I have read, understood and will comply with the provisions within this Code of Conduct. Understand that any breach of the Code of Conduct could result in disciplinary action by Salford Royal (or my own Trust/Company) and termination of access to the system.

First Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Surname: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Job Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Organisation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_