**PCIG Consulting Template**

**System Administrator Policy**

**Version: 4.0**

**Date: 31 March 2021**

**This template is for use by Practices to Comply with the UK GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.**

**Change Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **To** | **Change** | **Date** |
| **1** | **2** | **Reformatting and spelling corrected** | **26 July 2019** |
| **2** | **3** | **Reviewed and updated** | **1 May 2020** |
| **3** | **4** | **Reviewed and updated** | **31 March 2021** |

[Practice Name]

**System Administrator Policy**

**Document History**

|  |  |
| --- | --- |
| Document Reference: | … |
| Document Purpose: | This policy sets out the [practice name] expectations for the Practice employees who have administration and access rights to the electronic communications, files, or documents of the Practice and have Administrator level access.  |
| Date Approved: | 31 March 2021 |
| Version Number: | 4.0 |
| Status: | FINAL |
| Next Revision Due: | March 2022 |
| Developed by: | Paul Couldrey – IG Consultant |
| Policy Sponsor: | Practice Manager |
| Target Audience: | This policy applies to any person directly employed, contracted, working on behalf of the Practice or volunteering with the Practice. |
| Associated Documents: | All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2021 |

1. **Introduction**

The purpose of this policy is to establish the Practice’s expectations for the Practice employees who have administration and access rights to the electronic communications, files, or documents of the Practice and have Administrator level access.

1. **Definitions**

For the purposes of this policy, the term “Electronic Communications Systems” includes, but is not limited to, the use of Practice computer networks, the Internet, electronic mail (e-mail), telephones (including cellular telephones), voice mail, pagers, modems, fax transmissions, video, multimedia, and all other computer-related communications provided by the Practice. Facilities, technologies, and information resources used for Practice information processing, transfer, storage and communications are also included.

1. **Responsibilities of System Administrators**

The creation and operation of electronic communications systems require personnel to configure, manage, administer, and monitor computer and other electronic communications hardware and software. System administrators who configure these systems and services and monitor the performance of these systems are responsible for:

* Setting up accounts for individuals to access information and services
* Helping resolve problems with usernames and passwords
* Researching and resolving problems
* Configuring systems and services to the needs of the organization
* Monitoring the performance of systems and services
* Taking corrective action to improve performance
* Implementing corrections and upgrades to provide new features and enhancements
* Identifying internal and external risks to the security, confidentiality, and integrity of information
* Evaluating the effectiveness of the current safeguards for controlling security risks
* Designing and implementing a safeguards program
* Regularly monitoring and testing the safeguards program

1. **Access to Electronic Communications and Files**

All hardware and software associated with the electronic communications systems are the property of the Practice. The Practice supports a climate of trust and respect and does not ordinarily read, monitor, or screen electronic mail or other electronic data, files or records. However, the Practice retains the right, in circumstances described below, to access electronic communications, data, files or records for Practice related purposes and members of the Practice community should therefore have no expectation of privacy with respect to the use of electronic resources.

Employees and agents of the Practice may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and permission to access the confidential contents.

System administrators of the Practice may read, listen to or otherwise access confidential electronic communications, including e-mail, and electronic data, files or records, provided that the employee or agent needs to access the confidential contents in order to perform the responsibilities of his or her job and access is necessary to maintain system integrity, including but not limited to, tracking viruses and performing ordinary system repair, maintenance and enhancement.

1. **Responsibilities Defined as: -**

System Administrator Responsibilities: As part of normal business processes and practices, Network Administrators are:

* Held to the highest standard of behaviour and ethics because they have the capability and responsibility to maintain system integrity and must be trusted with the security and privacy of all data on the network.
* Allowed access to users' private information and, as such, are required to protect the privacy, confidentiality and integrity of this information always.
* Expected to take every reasonable effort to safeguard services and data stored on the Practice network. Administrators are not liable for any loss of data or loss of service on the Practice network. The ultimate responsibility for safeguarding data rests with the user through proper security and archival procedures.
* Required to notify the partners and their supervisors of any observed violations of Practice computing policies, licensing agreements with software manufacturers, or observed violations of practice policies regarding these matters.
* Charged with investigating policy violations and suspected abuse of computing resources. Where violations of a policy occur, Administrators are authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system.
* During such investigations, Administrators may inspect any data files and may monitor network traffic.
* Required to follow the Practice Policy on Security Incident Response Policy
* Follow additional responsibilities to the Practice as a whole, regardless of the policies of Practice and ICT Services Provider.
1. **Best Practice**

The following best practices will be followed as part of normal business processes and practices:

* Disaster recovery plans of critical systems and services will be developed and reviewed on an annual basis. All administrators will become familiar with the plan. Key systems and services will be tested against the disaster plan on a regular basis as determined by the Administrators. A copy of the plan will be stored on the department SharePoint site and a backup copy will be stored securely offsite.
* File and data backup plans will be kept and followed for all systems and services.
* Backup media will be stored off-site to minimize risk. All media will be rotated and destroyed on a regular basis.
* All system passwords will be changed on an annual basis. Safe password guidelines will always be followed.
* Log files on critical systems will be reviewed regularly for possible intrusion detection. Automated processes will be developed and used whenever possible in order to filter out actual abuses and to keep the review window as short as possible, ideally every day.
* Administrators will never authenticate to critical devices or services with administrative rights when performing non-administrative tasks.
* All network and systems changes, no matter how trivial the change may appear, will go through a written peer review process with change logs that includes a plan for migrating development environments into production environments.
* Every attempt will be made to adopt the latest advances in security hardware, software and methods that do not interfere or restrict the teaching, learning and research mission of the Practice School or it’s community of faculty, staff, students and alumni.
* Permission must be obtained from the Partners before access to sensitive data is granted to any Practice person outside of the department that owns the data.
* Maintain the application software in a fully supported version with all appropriate patches and updates via the Practice Information Asset Register
* Configure and maintain the systems, software and end-user computers in a way that optimizes security.

1. **Job Related Duties**

 Administrators will use reasonable efforts to:

* Take precautions against theft of or damage to the system components.
* Faithfully comply with the terms of all hardware and software licensing agreements.
* Become familiar with all applicable Practice and Practice policies.
* Participate in required Administrator training
1. **Signature**

BY signing this policy, I agree to the responsibilities and rights of a system administrator for [Practice Name] and will comply with the requirements above and affirm that I will conduct my duties to the highest standard of use.

Signature: ………………………………………………

Name: ………………………………………………

Position: ………………………………………………

Date: ………………………………………………

Review Date: ………………………………………………

Caldicott Guardian Authorisation: ………………………………………………

Caldicott Guardian Name: ………………………………………………

Date: ………………………………………………