**DARWEN HEALTHCARE**

**Darwen Healthcare**

**Data Security & Protection (Information Governance)**

**Policy R028**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version:** | **Review date:** | **Edited by:** | **Approved by:** | **Comments:** |
| 1 | 01 June 2022 | Ann Neville | GP Partners | Policy Reviewed |

|  |  |
| --- | --- |
| Policy Number / Version | Final v4.0 June 2022 |
| Ratified by |  |
| Date ratified |  |
| Name of originator/author | Ann Neville/Philip Cribb |
| Date issued |  |
| Review date |  |
| Date of first issue |  |
| Scope | All staff, including temporary staff and contractors |

**CONSULTATION AND RATIFICATION SCHEDULE**

|  |
| --- |
|  |
| **Name of Team ratifying Policy** | **Date of ratification** |
| Caldicott Guardian & IG Lead |  |
| SIRO | **June 2022** |
|  |  |
|  |  |
|  |  |

1. **Introduction**

Information is a vital asset, both in terms of clinical management of individual patients and the efficient planning and management of services and resources. It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

This policy provides assurance to Darwen Healthcare and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. Darwen Healthcare will establish and maintain this policy and the associated procedures to ensure compliance with the requirements of: -

* The Data Security & Protection (DSP) Toolkit (formerly the Information Governance Toolkit)
* The UK Data Protection Act (DPA) 2018
* The UK General Data Protection Regulation (UK GDPR) 2021
* The National Data Guardian Security Standards

This policy and its supporting procedures are fully endorsed by the Darwen Healthcare Partners.

1. **Scope**

This policy covers all aspects of information within the organisation, including but not limited to:

Patient/client/service user information, i.e.: -

• Personal Information (including ‘special category’ health information as defined by UK GDPR)

• Organisational Information

This policy covers all aspects of handling information, including but not limited to:

• Structured record systems – paper and electronic

• Transmission of information – fax, email, other forms of electronic transmission such as post and telephone

This policy covers all information systems purchased, developed and managed by or on behalf of Darwen Healthcare, and any individual directly employed or otherwise by Darwen Healthcare.

The key component underpinning this policy is the annual action plan arising from a baseline assessment against the standards set out in the NHS Digital Data Security and Protection Toolkit.

This policy cannot be seen in isolation as information plays a key part in corporate governance, strategic risk, clinical governance, Caldicott principles, service planning, performance and business management. This policy therefore links into all these aspects of Darwen Healthcare and is reflected in respective strategies/policies.

1. **Principles**

Darwen Healthcare recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

Darwen Healthcare fully supports the principles of corporate governance and recognizes its public accountability. It equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

Darwen Healthcare 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.

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

1. **Key Interlinked Themes of the Data Security and Protection policy:**

• Openness and Transparency

• Legal Compliance

• Information Security and Risk

• Quality Assurance

* 1. **Openness & Transparency**
* Darwen Healthcare recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
* Patients have access to information relating to their own health care, options for treatment and their rights as patients. There are clear procedures and arrangements for handling queries from patients and the public.
* Darwen Healthcare has clear procedures and arrangements for liaison with the press and broadcasting media.
* Integrity of information is developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
* Availability of information for operational purposes is maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.
* Darwen Healthcare regards all identifiable information relating to patients as confidential. Compliance with legal and regulatory framework is achieved, monitored and maintained.
* Darwen Healthcare regards all identifiable information relating to staff as confidential except where national policy on accountability and openness requires otherwise.
* Darwen Healthcare ensures that when person identifiable information is shared, the sharing complies with the law; guidance and best practice and both service users’ rights and the public interest are respected.
* Non-confidential information relating to Darwen Healthcare and its services is available to the public through a variety of media, in line with the Freedom of Information Act and Environmental Information Regulations.
* Data Security and Protection training including awareness and understanding of UK GDPR, Caldicott principles and confidentiality, information security, records management and data protection is mandatory for all staff. Data Security and Protection is included in induction training for all new staff.
	1. **Legal Compliance**
* Darwen Healthcare regards all identifiable information relating to patients as **confidential**.
* Darwen Healthcare will undertake or commission annual assessments and audits of its compliance with legal requirements via use of, and compliance with, the DSP Toolkit.
* Darwen Healthcare regards all person identifiable information relating to staff as **confidential**, except where national policy on accountability and openness requires otherwise.
* Darwen Healthcare maintains policies and procedures to ensure compliance with the Data Protection Act, UK GDPR, Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act and Environmental Information Regulations.
* Darwen Healthcare maintains procedures 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).
* Darwen Healthcare has a comprehensive range of procedures supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate.
	1. **Information Security and Risk**
* Darwen Healthcare maintains procedures for the effective and secure management of all information assets and resources.
* Darwen Healthcare will undertake or commission annual assessments and audits of its information and IT security arrangements via use of, and compliance with, the DSP Toolkit.
* Darwen Healthcare will promote effective confidentiality and security practice to its staff through procedures and training.
* Darwen Healthcare maintains incident reporting procedures and monitors and investigates all reported instances of actual or potential breaches of confidentiality and/or security.
* Darwen Healthcare maintains Risk Management and reporting procedures and has in place risk control and monitoring of all reported information risks.
	1. **Information Quality Assurance**
* Darwen Healthcare maintains procedures for information quality assurance and the effective management of records.
* Darwen Healthcare will undertake or commission annual assessments and audits of its information quality and records management arrangements via use of, and compliance with, the DSP Toolkit.
* Darwen Healthcare ensures that information is managed throughout its lifecycle of creation, retention, maintenance, use and disposal so that it is accurate, up to date, secure, retrievable and available when required.
* Employees take ownership of, and seek to improve, the quality of information within their services.
* Information quality is assured at the point of collection.
* Darwen Healthcare promotes information quality and effective records management through procedures and training.
1. **Responsibilities**
	1. **Caldicott Guardian/IG Lead/Practice Manager**

To define the Darwen Healthcare policy in respect of Data Security and Protection, taking into account legal and NHS requirements. The Partners are responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

* 1. **The Data Security & Protection (Information Governance) Lead**

Has overall accountability and responsibility for Data Security and Protection in Darwen Healthcare and is required to provide assurance, through the Annual Governance Statement that all risks to Darwen Healthcare including those relating to information, are effectively managed and mitigated.

* 1. **The Senior Information Risk Owner (SIRO)/Practice Manager**

The SIRO understands how the strategic business goals of Darwen Healthcare will be impacted by information risks. The SIRO acts as an advocate for information and will provide written advice to the DSP/IG Lead about the content of their Annual Governance Statement in regard to information risk. The SIRO provides an essential role in ensuring that identified information security threats are followed up and incidents managed. The SIRO ensures that the Partners are kept up to date on all information risk issues. The role is supported by the Reception Supervisor and two Senior Receptionists but the Risk assessment process will remain with the SIRO.

* 1. **The Caldicott Guardian.**

The Practice has an identified Caldicott Guardian. The Caldicott Guardian has responsibility for ensuring that all staff comply with the Caldicott Principles and the guidance contained in the Health and Social Care Information Centre’s (NHS Digital) document – “A Guide to Confidentiality in Health and Social Care”.

<https://digital.nhs.uk/article/1226/A-Guide-to-Confidentiality-in-Health-and-Social-Care->

The Caldicott Guardian guides the organisation on confidentiality and protection issues relating to patient information. This role is pivotal in ensuring the balance between maintaining confidentiality standards and the delivery of patient care. The Caldicott Guardian will also advise the Governing Body on progress and major issues as they arise.

* 1. **The Practice Manager**

The Practice manager is responsible for overseeing day to day Data Security and Protection issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Data Security and Protection within Darwen Healthcare.

* 1. **The Data Protection Officer**

The Data Protection Officer (DPO) will develop expert knowledge of data protection law and practices and provide support, advice and assurance to all staff regarding information handling compliance obligations. The DPO will also monitor compliance via involvement with the annual completion of the DSP Toolkit return.

*(See Appendix A)*

* 1. **All Management Staff**

Senior staff are responsible for ensuring that the policy and supporting procedures are built into local processes to ensure on-going compliance. Managers are also responsible for ensuring that staff attend, or complete locally, mandatory awareness training and refresher training as required.

* 1. **All staff**

 Whether permanent, temporary or contracted, all staff are responsible for ensuring that they are aware of the requirements incumbent upon them regarding information security and confidentiality and for ensuring that they comply with these on a day to day basis.

1. **Training/Awareness**

Data Security and Protection is part of the induction process. All new and existing staff receive annual mandatory training and guidance including Caldicott and confidentiality, data protection, information security, data quality, records retention and Freedom of Information.

1. **Monitoring/Audit**
* Darwen Healthcare monitors this policy and related strategies and procedures through the Partners Meeting.
* An assessment of compliance with the requirements of the Data Security and Protection Toolkit is undertaken each year. Darwen Healthcare identifies staff to undertake Administrator, Reviewer and User roles as described in the Toolkit.
* Annual reports and proposed action/development plans are presented to the Caldicott Guardian/DSP-IG Lead/SIRO for approval prior to submission of the Toolkit.
* Darwen Healthcare ensures that the support infrastructure for the SIRO is in place, and is kept under regular review.
1. **DSP/Information Governance Management**

DSP/Information Governance management across the organisation is co-ordinated by the ‘IG Group’. The responsibilities of the IG Group *(Caldicott Guardian, SIRO, IG Lead, DPO)* include, but are not limited to:

* Recommending policies and procedures to the Partners for approval.
* Recommending the annual submission of compliance with requirements in the DSP Toolkit and related action plan to the Partners for approval.
1. **DSP/Information Governance Improvement Plan**

The DSP/IG Lead, Practice Manager (SIRO) and DPO are responsible for monitoring the improvement plans and associated progress. The improvement plan (or ‘Working Document’) is fundamental to the organisation achieving compliance with the DSP Toolkit. It is essential that the Partners are updated on the progress of the plan and of any associated risks which will affect the organisations ability to achieve DSP Toolkit compliance.

1. **Review**

This policy and associated strategy and procedures will be reviewed on an annual basis or earlier if appropriate, to take into account any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

1. **Supporting Procedures**
* Information Governance Handbook Parts 1 & 2.
* Work Programme (See Appendix B)

**Appendix A – Data Security and Protection/Information Governance Framework**

|  |  |  |
| --- | --- | --- |
|  | Requirement | Detail |
| Senior Roles within Darwen Healthcare |  |  |
| DSP/IG Lead | Data Security & Protection (Information Governance)Organisational Lead: Governance, Performance and Risk | The key purpose of the role is to ensure Darwen Healthcare successfully implements a range of policies, processes, monitoring audits, training and awareness mechanisms to ensure a high level of compliance with Information Governance & Information Security. The post holder will ensure the implementation of corporate standards and a consistent organisation wide approach to Information Governance & Information Security. The DSP/IG Lead has overall accountability and responsibility for Data Security& Protection (Information Governance) and is required to provide assurance through the Annual Governance Statement that all risks to the organisation, including those relating to information, are effectively managed and mitigated. |
| Senior Information Risk Owner: | The Senior Information Risk Owner (SIRO) is the Practice Manager | The SIRO is expected to understand how the strategic business goals of Darwen Healthcare may be impacted by information risks. The SIRO will act as an advocate for information risk and will provide written advice to the Partners on the annual report in regard to information risk. The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed and that Partners are kept up to date on all information risk issues. The SIRO will be supported by the Operations Lead, Quality Lead and Patient Engagement Lead. |
| Caldicott Guardian | Caldicott Guardian: Dr M Umer | Darwen Healthcare Caldicott Guardian has particular responsibility for reflecting patients’ interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian will advise on lawful and ethical processing of information and enable information sharing. |
| Data Protection Officer | Philip Cribb | To provide support, advice and assurance on compliance obligations; to maintain expert knowledge of data protection law and practices and how they apply to the Practice; to monitor compliance with GDPR and Practice policies, including staff awareness and provisions for training;  |
|  |  |  |
| Data Protection Officer for GPs/CCGs | Hayley Gidman | mlcsu.dpo@nhs.net |
| **Key Policies** Policies set out the scope and intent of the organisation in relation to the management of Data Security & Protection (Information Governance) | **Ratification Schedule:** | **Partners** | **Policy Group** |
| **Data Security & Protection (Information Governance) Policy** | Jun 21 | Risk |
| **Data Security & Protection (Information Governance) Handbook** | Jun 21 | Risk |
| Policies are communicated to all staff via email, GP Teamnet and Hard Copy Files stored in Reception |
| **Resources** Details of key staff roles | **Dedicated** **Information** **Governance** **Staff** | Caldicott Guardian – Dr M Umer Email: mohammed.umer@nhs.net Practice Manager – Ann Neville Email: Ann.Neville1@nhs.net Data Protection Officer – Philip CribbEmail: Philip.Cribb@nhs.net |
| **Governance** **Framework** Details of how responsibility and accountability for IG is cascaded through the organisation. | **Information Asset Owners** | Information Asset Owners are senior individuals (Operations Lead) involved in the day to day operation of Darwen Healthcare The IAOs role is to: - Understand and address risks to the information assets they ‘own’; and - Provide assurance to the SIRO on the security and use of these assets.  |
| **Information** **Asset** **Administrators**  | The Information Asset Administrators (Patient Engagement Lead) will: - Ensure that policies and procedures are followed - Recognise potential or actual security incidents - Consult their IAO on incident management - Ensure that information assets registers are accurate and maintained up to date. Information Asset Owners have received specialist information risk training to allow them to be effective in their role.  |
| **Training and** **Guidance**Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receive training appropriate to their roles should be detailed. | **DSP/IG** **Handbook Parts 1 & 2** | Purpose of the Handbook: To inform staff of all aspects of data security and protection including the need for keeping information confidential• To inform staff about what is expected of them • To protect the Organisation as an employer and as a user of confidential information The Handbook has been written to meet the requirements of: • The Data Protection Act 2018 • UK GDPR 2021•The Human Rights Act 1998 • The Computer Misuse Act 1990 • The Copyright Designs and Patents Act 1988 • A Guide To Confidentiality in Health and Social Care (HSCIC) The Handbook has been produced to protect staff by making them aware of the correct procedures to follow to prevent any inadvertent breach. If the Handbook is breached then this may result in legal action against the individual and/or Organisation as well as investigation in accordance with the Organisation’s disciplinary procedures. The Handbook is available to all staff working for Darwen Healthcare and they acknowledge that they have received and understand the document. New starters to the organisation receive a copy of this with their contract. Both should be signed and returned to their line manager and kept on file. |
|  | **Training for all staff** | All staff receive basic DSP/IG training, initially via the online training tool offered by Blue Stream Academy. |
|  | **Specialist DSP/IG training** | As required specialist DSP/IG training is provided across the organisation for staff with additional responsibility for DSP/IG within their areas. Current specialist training includes: Information Risk Training Privacy Impact Assessments Caldicott and Data Protection Training |
| **Incident** **Management** Clear guidance on incident management procedures should be documented and staff should be aware of their existence, where to find them, and how to implement them.  | **Documented Procedures and Staff Awareness** | Incident Management in the CCG is covered in the following organisational policies and Procedures: • Incident and Accident procedure • DSP/IG Policy • DSP/IG Handbook Staff awareness is raised through the following ways: • Staff Induction • DSP/IG Training • Information Risk Training * Caldicott and Data Protection Training
 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **APPENDIX B – WORK PROGRAMME**

|  |  |  |  |
| --- | --- | --- | --- |
| **DSP/IG work stream** | **Requirement**  | **Work to achieve action**  | **Target date**  |
| **DSP/IG Training** **Lead: IG Group**  | All current staff to have completed Refresher DSP/IG & GDPR training. | Online training or face to face training held annually.Training to include information relevant to departments and staff attending the training session.Relevant DSP/IG questions asked of staff throughout the training sessions to gauge staff knowledge | 30/06/2022 |
| All new staff to complete DSP/ IG training. | Training to be completed via the DSP/IG online training tool | Within four weeks of the employees start date |
| Specialist training to be completed, including SIRO, Caldicott Guardian, Data Protection Officer and line managers | To complete annual training via Bluestream Academy | Annually |

|  |  |  |  |
| --- | --- | --- | --- |
| DSP/IG policies and proceduresLead: DPO/IG Group | Up to date DSP/ IG policy and handbook containing all relevant information that staff are required to understand | Policy and guidance created via IG Lead, DPO and Practice Manager | 30/06/2022 |
| Information Governance Promotional & Communication CampaignLead: Information Governance | Raise the profile of DSP/IG | Think Posters placed on notice boardsInformation placed on Team Briefs | Ongoing through the year |
| Increase communication about DSP/IG matters within Darwen Healthcare | Produce DSP/IG update reports and place on regular Team Brief | DSP/IG content on each Team Brief |
| Consult with staff in relation to the quality of the communications they receive | Use surveys to understand staff perception of DSP/IG and the general satisfaction levels in relation to DSP/IG communications | 31/12/2022 |
| Shared drive and records management standardsLead: Information Governance | Records to be stored appropriately on shared practice drive | Ensure folders are held in the appropriate area of the GP Teamnet | Ongoing updates |
| Work with the Practice Manager to develop best practice guidelines for staff on records management practices, including; folder naming, version control, retention and destruction | Work together to understand whether the practice is to raise awareness of records management best practice or whether to impose the records management standards as policy. Approval and circulation of appropriate policies | On-going |

|  |  |  |  |
| --- | --- | --- | --- |
| Audits Lead: Practice Manager/Corporate Governance Administrator | Information security spot checks and information security audits | Carry out regular information security spot checks.Support the ISO in the implementation of any remedial action as a result of the audit findings | Ongoing through the year |
|  | Confidentiality audits | Support the Practice Manager in the implementation of any remedial action as a result of the confidentiality audit findings | On-going through the year |
| IncidentsLead:Practice Manager | Ensure incidents are identified, recorded and acted upon in a timely and efficient manner | Ensure all Darwen Healthcare incidents including near misses are reported within 72 hours of their occurrence via the IG Toolkit reporting tool.Notify DSP/IG Lead/Caldicott Guardian and Partners of level 2 incidents. Ensure that a brief investigation is carried out for all level 0 and level 1 incidents and near misses. Offer support to Practice Manager in the investigation of level 2 incidents  | Ongoing through the year |
| Reports Lead:Practice Manager | SIRO report | Complete annual report to IG Lead | TBC |

 |
|  |
|  |