NHS
Dorset
Clinical Commissioning Group

NHS Dorset Clinical Commissioning Group

Data Security and Protection Policy

June 2018

Supporting people in Dorset to lead healthier lives



PREFACE

This policy sets out best practice guidance for all staff in managing information securely, legally and ethically.

All managers and staff (at all levels) are responsible for ensuring that they are viewing and working to the current version of this procedural document. If this document is printed in hard copy or saved to another location, it must be checked that the version number in use matches with that of the live version on the CCG intranet.

All CCG procedural documents are published on the staff intranet and communication is circulated to all staff when new procedural documents or changes to existing procedural documents are released. Managers are encouraged to use team briefings to aid staff awareness of new and updated procedural documents.

All staff are responsible for implementing procedural documents as part of their normal responsibilities, and are responsible for ensuring they maintain an up to date awareness of procedural documents.

A	SUMMARY POINTS
•	Policy and best practice guidance for managing information ethically, securely and legally

B	ASSOCIATED DOCUMENTS
•	Procedure for the Management of Adverse Incidents
•	Procedure for the Management of Serious Incidents
•	Remote Access and Off-Site Working Policy
•	IT Security Policy
•	Network Security Policy
•	Confidentiality: Staff Code of Conduct
•	Freedom of Information Policy
•	Data Security by Design and by Default

C	DOCUMENT DETAILS
Procedural Document Number	
Author	Paddy Baker /Helen Williams
Job Title	DPO/ DSP Manager
Directorate	Finance
Recommending committee or group	Information Asset Owners Group
Approving committee or group	Information Asset Owners Group
Date of recommendation (v1)	19 June 2018
Date of approval (v1)	19 June 2018
Version	1.3
Sponsor	Chief Finance Officer
Recommendation date	22 April 2020
Approval date	18 May 2020
Review frequency	Annually
Review date	18 May 2021

D	CONSULTATION PROCESS		
Version No	**Review Date**	**Author and Job Title**	**Level of Consultation**
1.3	27 March 2020	Paddy Baker, DPO Lynda Bennett, DSP Officer	Information Asset Owners Group, Information Security Manager, Head of Patient and Safety Risk

E	VERSION CONTROL				
Date of issue	**Version No**	**Date of next review**	**Nature of change**	**Approval date**	**Approval committee /group**
19 June 2018	1.0	19 June 2019	Updated to incorporate GDPR Requirements	27 March 2020	Information Asset Owners Group
19 June 2019	1.2	19 June 2020	Review	19 June 2020	Information Asset Owners Group
18 May 2020	1.3	18 May 2021	Updated to incorporate password policy and minor amendments	18 May 2020	Directors Performance Committee

F	SUPPORTING DOCUMENTS/EVIDENCE BASED REFERENCES	
Evidence	**Hyperlink (if available)**	**Date**
Information Governance Review		2013
National Data Guardian for Health and Care – Review of Data Security, Consent and Opt-Outs		2016
NHS Code of Practice: Records Management	www.opsi.gov.uk	2006 updated 2009
Records Management Code of Practice for Health and Social Care	www.opsi.gov.uk	2016
NHS Code of Practice – Information Security Management	www.opsi.gov.uk	2009
NHS Code of Practice: Confidentiality	www.opsi.gov.uk	2003
HSG(96)18 – The Protection and Use of Patient Information		1996
HSC 1999/012 – Caldicott Guardians		
HSC 2002/003 – Implementing the Caldicott Standard into Social Care		2002
The Caldicott Principles	www.gov.uk	1997
The Caldicott 2 Review	www.gov.uk	2013

F	SUPPORTING DOCUMENTS/EVIDENCE BASED REFERENCES	
Evidence	**Hyperlink (if available)**	**Date**
Data Protection Act	www.opsi.gov.uk	2018
General Data Protection Regulations		2018
Human Rights Act	www.opsi.gov.uk	1998
Access to Medical Reports Act	www.opsi.gov.uk	1988
Freedom of Information Act	www.opsi.gov.uk	2000
Department of Health Guidance for Access to Health Records Requests		2010
Common Law Duty of Confidentiality	www.opsi.gov.uk	
Electronics Communications Act	www.opsi.gov.uk	2000
Computer Misuse Act	www.opsi.gov.uk	1990
Civil Contingencies Act	www.opsi.gov.uk	2004
Health and Social Care Act	www.opsi.gov.uk	2001 updated 2015
Protocol for Information Sharing between Health & Social Care Agencies		2006
National Archives Guidelines on Developing a Policy for Managing Email	www.nationalarchives.gov.uk	2004
Public Records Act	www.opsi.gov.uk	1958
NHS Constitution	www.gov.uk	2015
HSCIC Guide to Confidentiality in Health and Social Care: Treating Confidential Information with Respect	www.digital.nhs.uk	2013
HSCIC Code of Practice on Confidential Information	www.digital.nhs.uk	2014
Security of Network Information Systems Regulations (NIS)		2018

G	DISTRIBUTION LIST		
Internal CCG Intranet	**CCG Internet Website**	**Communications Bulletin**	**External stakeholders**
√	√	√	

1. RELEVANT TO

1.1 This policy and associated strategy, guidance and procedures applies to all staff within the CCG whether operating directly or providing services under a service level agreement or joint agreement. The policy is relevant to all staff including contracted employees, lay members and contracted third parties such as bank, agency, volunteers, locums, student placements, staff on secondment, researchers, visiting professionals and suppliers.

2. INTRODUCTION

2.1 Effective Data Protection requires clear management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation is measured against effective implementation of data protection is through achievement of the Data Security and Protection Toolkit (DSPT).

2.2 Data Security and Protection (DSP) policies must be approved at the most appropriate senior management level in the organisation and be reviewed annually.

2.3 The main pieces of legislation are the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation 2016 (GDPR).

2.4 Other legislation that protects confidential information is:

- Article 8 of the Human Rights Act 1998. Everyone has the right to respect for his private and family life, his home and his correspondence;
- The Common Law Duty of Confidentiality. A duty of confidence arises when one person discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence.

2.5 The CCG fully supports the principles of data protection and recognises its public accountability, but equally places importance on the confidentiality of personal information, and the security arrangements in place to safeguard that information and also any commercially sensitive information.

2.6 The CCG 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.

3. SCOPE

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

- patient information;

- workforce information;
- organisational information;
- information from a third party, held or processed by the CCG.

4. PURPOSE

4.1 The purpose of this document is to set out the process, governance arrangements, strategy and policy framework for the delivery of safe and effective data protection within the CCG and for any services commissioned by the CCG.

5. DEFINITIONS

5.1 A list of definitions, terms and abbreviations used in this document can be found within the glossary at **Appendix A**.

6. ROLES AND RESPONSIBILITIES

Governing Body

6.1 It is the role of the Governing Body to define the CCG policy in respect of data protection, taking into account legal and NHS requirements. The CCG Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of this policy.

6.2 The CCG Governing Body, whilst retaining their legal responsibilities, has delegated data protection compliance to the nominated Data Protection Officer (DPO), Caldicott Guardian, Senior Information Risk Owner (SIRO), and the Information Asset Owners Group (IAOG).

Chief Officer

6.3 The Chief Officer is the named officer with responsibility for ensuring that the CCG complies with its statutory obligations and Department of Health directives for data protection. The Chief Officer is required to provide assurance through the Statement of Internal Control (SIC) annually that all risks relating to information are effectively managed. The Chief Officer also ensures that the roles of SIRO and Caldicott Guardian are assigned and supported.

6.4 The Chief Officer will ensure that the CCG has access to specialist advice regarding the requirements of relevant legislation.

6.5 Responsibility for implementation of data protection, data quality, records management and information security has been delegated to the DPO.

Senior Information Risk Owner (SIRO)

6.6 The Chief Finance Officer is the SIRO for the CCG and is also the Director responsible for the Data Security and Protection team.

6.7 The SIRO attends all Governing Body meetings, acts as an advocate for information risk on the Governing Body and in internal discussions and provides written advice to the Chief Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk. The SIRO is responsible for authorising access to national systems.

6.8 The key responsibilities of the SIRO are to:

- oversee the development of an Information Risk Policy and a strategy for implementing the policy within the existing DSP Framework;
- take ownership of the risk assessment process for information and cyber security risk, including review of an annual information risk assessment to support and inform the SIC;
- review and agree action in respect of identified information risks;
- ensure that the organisation's approach to information risk is effective, in terms of resource, commitment and execution and that this is communicated to all staff;
- provide a focal point for the resolution and / or discussion of information risk issues;
- ensure the board is adequately briefed on information risk issues;
- ensure that all systems containing personal identifiable data are recorded as information assets on the CCG Information Asset Register and provide leadership and guidance to assigned Information Asset Owners.

6.9 The SIRO is supported by the DPO, the Data Security and Protection Advisory Team (DSPAT), the Information Security Manager (ISM) and the Caldicott Guardian.

Caldicott Guardian

6.10 The Director of Nursing and Quality is the Caldicott Guardian for the CCG and is responsible for protecting the confidentiality of people's health and care information and making sure it is used properly.

6.11 The Caldicott Guardian is responsible for advising the CCG and the Governing Body on confidentiality issues. This also includes establishing and maintaining procedures governing access to, transfer of, and the use of person confidential data held or processed within CCG systems.

6.12 The Caldicott Guardian is responsible for:

- ensuring compliance with the principles contained within the Confidentiality: NHS Code of Practice and ensuring that staff are made aware of individual responsibilities (and changes to the Caldicott principles), through policy, procedure and training;

- ensuring audit and monitoring of access to confidential information and systems.

6.13 The Caldicott Guardian for the CCG is supported by the DPO, the DSPAT, the Information Security Manager, the SIRO and the IAOG members.

7. SUPPORTING ROLES

Data Protection Officer (DPO)

7.1 The DPO is an advisory role supported by the DSPAT to provide guidance and specialist advice and support to the CCG on data security and protection.

7.2 The DPO's responsibilities include:

- informing and advising the CCG about complying with GDPR and the DPA 2018;

- monitoring compliance with GDPR and data protection laws – including staff training and internal audits;

- advising on and monitoring data protection impact assessments;

- overseeing investigations into information and cyber related incidents;

- co-operating with the ICO;

- being the first point of contact for the ICO and citizens in terms of data processing.

7.3 The DPO has overall responsibility for co-ordinating the DSP work programme and completion of the annual assessment.

7.4 Responsibility for Freedom of Information (FOI) and for ensuring that all FOI processes are in place to comply with the Act has been delegated to the DPO, supported by the DSPAT. This includes ensuring the CCG FOI publication scheme is up to date and establishing appropriate arrangements to deal with appeals/investigations into complaints about decisions and response times.

7.5 The DPO is also responsible for records management within the CCG.

Information Security Manager (ISM)

7.6 The IM&T Infrastructure Manager is the ISM for the CCG and is responsible for co-ordinating the information security agenda for the CCG, supported by the Patient Safety and Risk Manager, the DPO, the DSPAT, the SIRO, the Caldicott Guardian and IAOG members.

7.7 The ISM is responsible for ensuring compliance with the information security components of this policy and the DSP Toolkit. This includes providing regular reports to the SIRO and to the IAOG.

7.8 The ISM is also responsible for administering the security of the information assets in accordance with ISO/IEC 17799.

7.9 The ISM is responsible for co-ordinating the necessary response and resolution activities following a suspected or actual cyber security incident or breach, and for providing advice and guidance.

Information Risk Lead

7.10 The Patient Safety and Risk Manager is responsible for feeding information risks into the organisation wide risk register.

7.11 Further responsibilities are to support the organisation in the risk assessment process, including the programme that considers the security risks to:

- information assets;
- transfers of information identified in the information flow mapping.

Business Continuity Lead

7.12 The Assurance Lead is responsible for ensuring that the organisation has a business continuity strategy and plans in place for all critical information assets identified in the Information Asset Register, and for obtaining approval of the plans from the SIRO.

7.13 Responsibilities also include ensuring the business continuity plans are regularly tested and the outcomes documented through simulation exercises.

Data Quality Lead

7.14 The Head of Business Intelligence is responsible for ensuring that systems and processes are in place to provide accurate and timely validation of information in relation to commissioned services, and for production and monitoring of the CCG's Data Quality policy.

Information Asset Owners Group (IAOG) Members

7.15 IAOG members provide day to day support to staff within their directorates on all aspects of DSP, and represent the directorate at the IAOG. They also develop, support and monitor the work programme to enable the DSPT to be completed on an annual basis.

7.16 IAOG members assist in the data security and protection audit programme and co-ordinate the reporting of any breaches in information security or compliance with DSP policies and procedures.

7.17 Members of the IAOG also:

- advise the Governing Body on issues relating to data protection, confidentiality and information security;

- offer support advice and guidance to the Caldicott Guardian and SIRO.

7.18 Terms of reference for the IAOG can be found at **Appendix B**.

Information Asset Owners (IAOs)

7.19 IAOs are responsible for ensuring that all information assets are appropriately owned and managed. The IAOs work with all members of staff in their directorates (and across directorates as appropriate) to ensure there is clear ownership and regular review of information assets and the mapping of data flows and the legal basis for the data flows to the information assets.

7.20 The IAOs must ensure that any system and users they are responsible for comply with the current DPA legislation.

7.21 The IAOs are responsible for ensuring that:

- the system is recorded on the Information Asset Register;

- users are set up on the system on a need to know basis in line with access control procedures;

- data flows of personal information are recorded for the information asset;

- records retention periods are set for records held on the system;

- expert advice is available regarding data protection issues;

- unusual requests for disclosure are scrutinised;

7.22 IAOs support the SIRO in managing the risk associated with all information assets.

Director of Engagement and Development

7.23 The Director of Engagement and Development is responsible for overseeing all staff requests for access to personal files, with support from the DSPAT.

7.24 The Director of Engagement and Development will ensure that appropriate clauses are in staff contracts to ensure that all staff are bound by the requirements of the Data Protection Act 2018.

Managers

7.25 Managers are responsible for ensuring staff are aware of all policies relating to DSP.

7.26 The day to day responsibility for enforcing this policy and associated documentation is delegated to Line Managers. Managers will ensure that all staff:

- attend appropriate training;
- know how to deal with requests for person identifiable information.

7.27 Managers are responsible for ensuring Data Protection Impact Assessments (DPIAs) are completed whenever a service is changed or a new project is started, in accordance with the CCG Guidance and Template available on the intranet.

Staff

7.28 All staff are expected to adhere to this policy and associated guidance on using and sharing of personal information. Any breaches of this policy will be investigated in line with the CCG disciplinary procedures.

7.29 All staff are required to attend DSP training on an annual basis.

7.30 All CCG employees are responsible for ensuring that all the personal data used and held by the CCG is secured from loss, corruption, damage and disclosure.

7.31 All staff who create, receive and use records are responsible at law for any records they create and use. Staff must be aware that any records they create are not their personal property but belong to the CCG.

8. KEY GOVERNANCE BODIES

Information Asset Owners Group (IAOG)

8.1 The CCG has established the IAOG comprising representatives from directorates within the CCG in order to promote a consistent approach to DSP. The group is responsible for developing and sharing best practice across the organisation and ensuring that DSP standards are included in other work programmes and projects.

8.2 The group co-ordinates the review of the CCG's DSP management and accountability arrangements and produces and monitors the annual DSP work programme. The CCG recognises that other key staff will be involved in, and contribute to, this work programme.

8.3 The group is responsible for reviewing, approving and monitoring DPIAs to ensure privacy considerations are taken into account when new projects are introduced or changes are made to existing services.

8.4 The group is also responsible for advising the Governing Body on issues relating to data protection, confidentiality and information security.

8.5 The IAOG reports to the Audit Committee, and responsibility for the approval of related policies and procedures is delegated to the Directors Performance Group on behalf of the CCG Governing Body.

8.6 Terms of Reference for the group were agreed by the IAOG on 19 June 2018 and can be seen at **Appendix B**. These are reviewed on an annual basis.

Formal Committee to Governing Body – Audit Committee

8.7 In line with CCG standing orders, a formal report on DSP is received by the Audit Committee on a quarterly basis.

8.8 Any policies and procedures agreed by the IAOG will be submitted to the Directors Performance Group for approval, before they are noted by the Audit Committee.

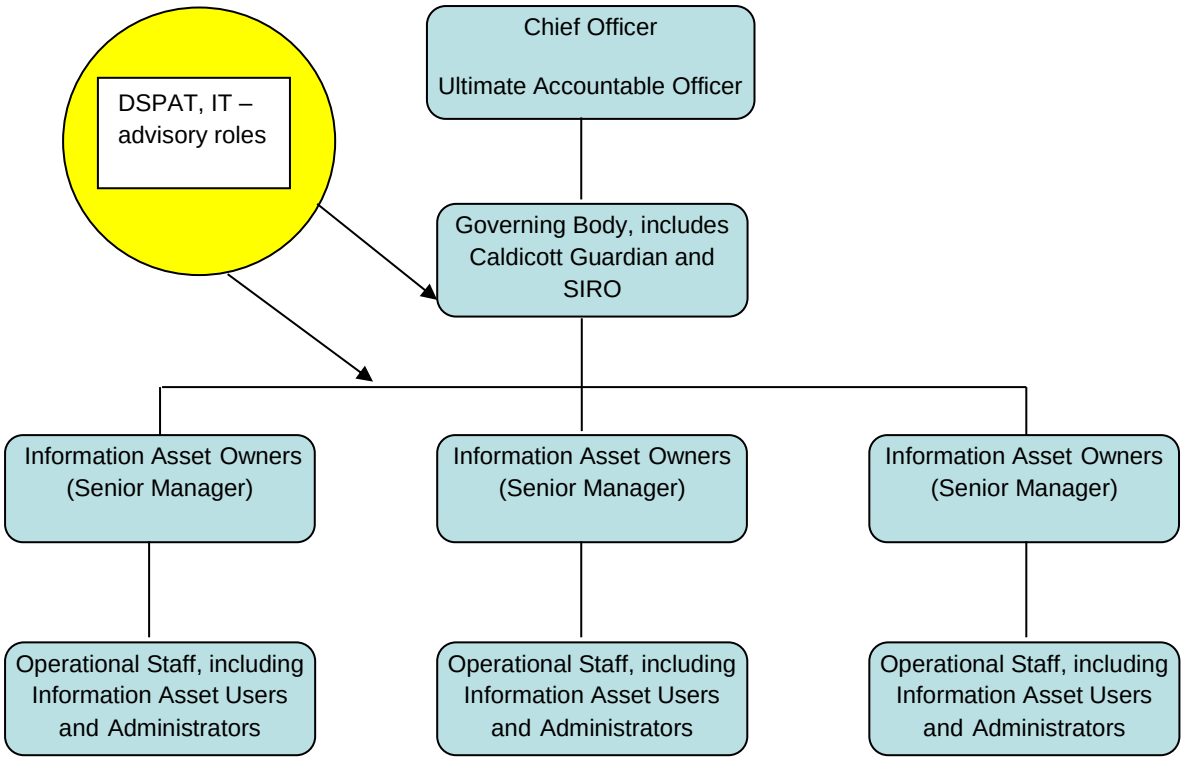
8.9 Any concerns raised by the Audit Committee will be highlighted to the Governing Body.

9. DATA SECURITY AND PROTECTION MANAGEMENT AND ASSURANCE

9.1 The CCG has established an approach to Data Security and Protection that ensures the organisation (from Governing Body level down) has the ability to comply fully with its requirements in terms of GDPR, data protection, confidentiality and information security. The roles and responsibilities that form part of this approach are set out above in sections 6 and 7 of this policy.

9.2 The governance arrangements in place to achieve assurance of compliance with DSP are set out below:

Overarching Approach to Data Security and Protection Assurance



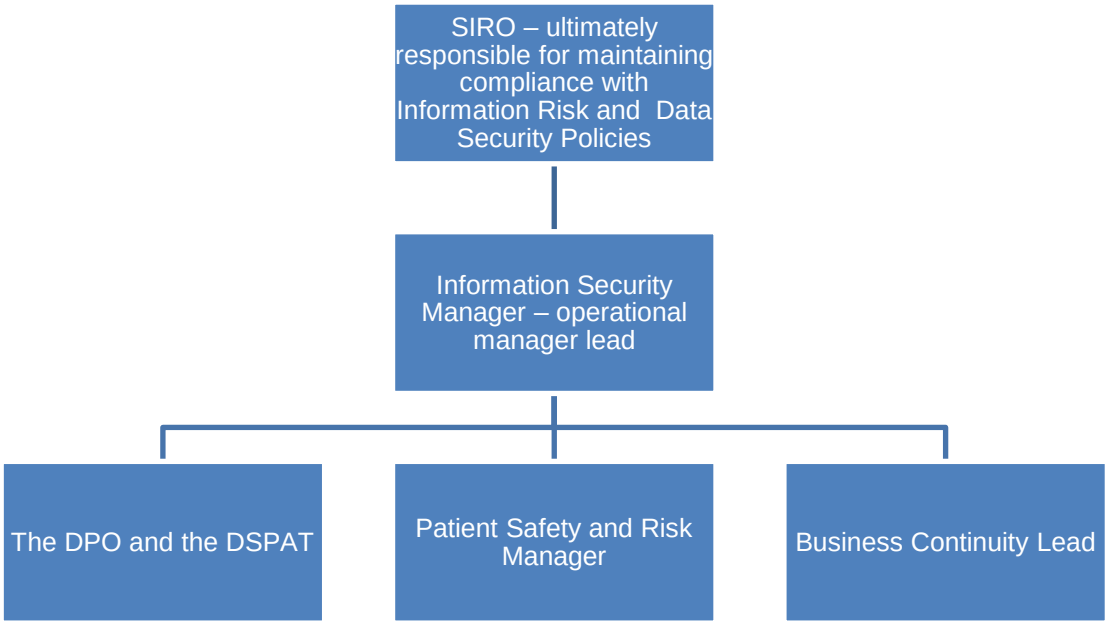
9.3 An information asset is defined by the national archives as: “a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles.”

9.4 The information systems, equipment, software and data used by the CCG represent a considerable investment and are valuable assets, essential to the effective and continuing operation of the CCG. Some of the data held by the CCG is of a confidential nature and it is necessary for this information and the information systems to be protected against any events, accidental or malicious, which may put at risk the activities of the CCG or their investment in information.

9.5 The CCG has an Information Asset Register in place to record all systems/information assets holding or sharing personal information. The register is maintained by the IAOs, and risks to the information assets are assessed, reviewed and reported to the SIRO. System security and access control is also managed by the IAOs, along with the mapping of information flows to and from the information assets to ensure information is kept secure.

9.6 Data Security Assurance in line with DSP requirements is formalised within information risk and data security policies and procedures under the leadership of the SIRO and the ISM, and embedded in the directorate structures of IAOs.

9.7 The relevant responsibilities for complying with and maintaining data security and risk are set out below:



9.8 Risks associated with any aspect of data security are entered onto the CCG Risk Register and managed locally to reduce them to the lowest possible level.

9.9 A risk assessment will be carried out for each of the CCG information systems by the IAO. Measures will be put in place to ensure each system is secured to an appropriate level.

9.10 Once identified, information security risks will be managed on a formal basis. Risks will be recorded within the CCG risk register and action plans put in place to demonstrate effective management of the risks.

9.11 The CCG is committed to maintaining and developing an infrastructure for information and information assets which has an appropriate level of security. All information assets will have a minimum security framework. In the case of local or standalone systems, it is the responsibility of the relevant manager to ensure compliance with this policy.

9.12 The CCG has also established business continuity and disaster recovery plans for critical information systems and networks.

10. COMMISSIONING OF SERVICES

10.1 The System Integration, Primary and Community Care and the Quality teams are additionally responsible for ensuring that DSP arrangements are in place and monitored in all organisations contracted to provide services to the CCG, either under a full contract or through a Service Level Agreement.

10.2 The CCG Contracting Team and the out-sourced Procurement Team, commissioned by the CCG, are responsible for ensuring that contracts with all third parties that handle personal information are compliant with GDPR before access is allowed to CCG information systems. These contracts must also ensure that the staff or subcontractors of the external organisation comply with all appropriate security policies.

10.3 The System Integration and the Primary and Community Care teams are responsible for ensuring that provider compliance with DSP is reviewed through contract monitoring, and that any new service developments with providers are subject to the completion of a DPIA, where applicable.

10.4 Formal procedural arrangements are in place to ensure that compliance with the commissioning/contract responsibilities outlined above is maintained and reviewed regularly.

10.5 Where there is an urgent requirement for a contactor to be on site at the CCG and it is not possible to agree a contract in time, individual line managers are responsible for ensuring that a Confidentiality Agreement is completed to enable the contractor to work freely without breach of confidentiality.

11. INCIDENT MANAGEMENT

11.1 The CCG has two sets of procedures in place for the management of all incidents, including security breaches and breaches of personal data. These are available on the CCG intranet:

- Procedure for the Management of Adverse Incidents;
- Procedure for the Management of Serious Incidents.

11.2 Under the GDPR, a personal data breach is defined as:

- a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

11.3 The Article 29 Working Party on personal data further defines three types of data breaches:

- **Confidentiality breach** – unauthorised or accidental disclosure of, or access to personal data;
- **Integrity breach** – unauthorised or accidental alteration of personal data;
- **Availability breach** – unauthorised or accidental loss of access to, or destruction of, personal data.

Data Breach Reporting

11.4 Staff must report all data breaches, whether suspected or actual, so that they can be investigated, appropriate actions taken to address the breach and lessons learnt so that they do not recur.

11.5 Breaches are reported through the CCG data breach reporting system found on the Data Security and Protection Intranet page. Data breaches are discussed at the DSP induction. High risk data breaches are reported via email to the DPO to ensure action is taken within the statutory timeframe.

11.6 Reports of data breaches are provided to the IAO group for review and discussion.

11.7 Externally commissioned services are reviewed at contract performance meetings, the timing of which are set by the CCG according to the complexity of activity of each provider organisation, and at least annually. The main Dorset NHS Foundation Trust meetings take place quarterly and the standard agenda includes a section on quality and outcomes where data security reviews and serious breaches are raised by exception.

11.8 If the CCG becomes aware of any breach of IT System security, including an actual, potential or attempted breach the CCG will inform any 3rd party suppliers or partners whose systems may be affected by the breach or attempted breach

Mandatory Reporting of Data Breaches

11.9 It is a legal obligation to notify the Information Commissioner of personal data breaches of the GDPR under Article 33, within 72 hours, unless it is unlikely to result in a risk to the rights and freedoms of others. Article 34 also makes it a legal obligation to communicate the breach to those affected without undue delay when it is likely to result in a high risk to individual's rights and freedoms.

11.10 The ICO has asked all relevant health and social care organisations to use the incident reporting tool accessed via the DSPT. Those breaches that also fulfil the criteria of a notifiable incident under the Security of Network Information Systems Regulations 2018 (NIS) will be forwarded to the Department of Health and Social Care, where the Secretary of State is the competent authority for the implementation of the NIS directive in the health and social care sector. The Information Commissioner is the national regulatory authority for the NIS directive.

11.11 The CCG maintains a record of all data breaches. If a data breach meets the reporting criteria it will be reported to the ICO.

12. DATA PROTECTION AND GDPR

12.1 The Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) 2016 applies to all person identifiable information about living individuals held in manual files, computer databases, videos and other automated media. This includes personnel, payroll records and other manual files.

12.2 The DPA defines six principles of good practice to follow when obtaining, processing, holding/storing personal data relating to living individuals. These are referred to as the 'data protection principles'.

12.3 The DPA also requires the CCG to register its data holdings with the Office of the Information Commissioner, identifying the purposes for holding the data, how it is used and to whom it may be disclosed. Failure to register or an incorrect registration is a criminal offence and may lead to the prosecution of the organisation.

Rights of Individuals

12.4 The DPA 2018 gives all living individual's additional rights. The CCG has documented guidance and procedures on managing these rights, including the right of subject access.

Transparency

12.5 In accordance with GDPR and FOI legislation, the CCG recognises the need for an appropriate balance between transparency and confidentiality in the management and use of information.

12.6 Information will be defined, and, where appropriate, kept confidential, in line with the revised Caldicott Principles and the principles outlined in the DPA 2018 and GDPR. Non-confidential information on the CCG and services will be available to the public through a variety of means, as set out in the FOI publication scheme.

Legal Compliance

12.7 The CCG considers all identifiable personal information relating to patients and staff as confidential (except where national policy on accountability and openness requires otherwise) and is committed to acquiring, using and storing information legally and ethically in line with legislation, policies and guidance.

12.8 The CCG also recognises that on occasions, legal and professional guidance may need to be sought for information security and disclosure issues. Applications for legal advice must be directed to the CCG solicitors through the DPO.

13. DATA PROTECTION IMPACT ASSESSMENTS (DPIAS)

13.1 A DPIA is a process to help identify and minimise the data protection risks of a project. A DPIA must be completed for any processing that is likely to result in a high risk to individuals.

13.2 The CCG has agreed the use of the DPIA template produced by the Information Commissioner's Office (ICO) and has produced a procedure to assist with identifying when a DPIA is required, and how to complete a DPIA. This can be found on the Data Security and Protection page on the CCG Intranet, along with a DPIA template form.

13.3 All DPIAs and accompanying action plans will be approved and monitored by the IAOG.

14. RECORDS MANAGEMENT

14.1 Records management is the process by which the CCG manages all aspects of records, whether internally or externally generated and in any format or media type, from their creation, through their lifecycle and eventual disposal.

14.2 Effective records management ensures that information is properly managed and is available whenever and wherever there is a justified need for information in accordance with the requirements of the GDPR.

14.3 The CCG has produced a Records Management and Retention Policy, with records management guidance. IAOs are responsible for producing records retention schedules for the teams within the directorate.

15. DATA QUALITY ASSURANCE

15.1 The quality of information acquired and used within the CCG is a key component to its effective use and management. As such, managers will be expected to take ownership of, and seek to improve, the quality of data collected and held within their services.

15.2 The CCG has produced a data quality policy and general guidance for staff. IAOs are responsible for ensuring that data quality procedures are in place for those information assets where personal data is collected, to ensure that wherever possible, information quality will be assured at the point of collection. This will include reference to nationally available systems such as SUS Data Quality Dashboards and Key Performance Indicator (KPI) reports, enabling commissioners to explore data quality issues across contracted provider services.

16. NHS CONSTITUTION

16.1 The CCG will abide by the rights and pledges made within the NHS Constitution, including:

- you have the right to be treated with dignity and respect in accordance with your human rights;
- you have the right of access to your own health records and to have any factual inaccuracies corrected;
- you have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure;
- you have the right to be informed about how your information is used;
- you have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

17. BRING YOUR OWN DEVICE (BYOD)

17.1 Staff are expressly prohibited from using personal devices (BYOD) to process any CCG data.

18. BRING YOUR OWN CLOUD/SERVICE

18.1 Staff are expressly prohibited from signing up to or using any cloud based service that has not been approved by the IAOG.

18.2 Use of peer to peer file sharing systems is not permitted as these may be unsecure and potentially breach GDPR and represent security risks. This includes BitTorrent, Dropbox, Limeware etc. If there is a requirement to share large files with third parties, this can be done securely via

https://securesend.dorsetccg.nhs.uk. If a third party asks to send data to the CCG via a file sharing process, then approval should be obtained from IT or DSPAT. The CCG has approved use of wetransfer for a limited set of users in the Engagement and Development Directorate and this service must not be used for sensitive information.

19. INFORMATION AND CYBER SECURITY

19.1 The CCG has established policies for the effective and secure management of its information assets and resources and works closely with other agencies that support this function by ensuring that staff have access to and are familiar with the information security policies and procedures.

19.2 Information security is addressed at recruitment stage for all staff and all contracts of employment and job descriptions include a confidentiality clause.

19.3 Where staff are unsure about sharing information, they should refer to the Confidentiality: Staff Code of Conduct, the Dorset Information Sharing Charter (DiSC), or take advice from the ISM, the DSPAT or the Caldicott Guardian.

Passwords and Access Control

19.4 Access to electronic information assets will be controlled on the basis of service requirements and managed through the use of procedures for allocating and controlling access, secure logins and passwords.

19.5 When choosing a password, rather than using a single long word that appears in a dictionary or a shorter word with numbers on the end, it is better to use a short phrase that won't appear in any dictionary. CCG policy allows this without being forced to use caps or numbers and so an effective password could be "thecatsatonthedog".

19.6 Words that are easily guessable such as a name, CCG, Dorset, NHS, password, secret, Vespasian, Canford, login etc. should not be used in a password. Whilst selecting a good password, a resource such as haveibeenpwned's password checker may be used.

19.7 A previous password must not be reused. When changing a password containing numbers these should not be cycled to the next number in the sequence. If a password is compromised, an attacker would be likely to try the same password with variations in the numbers.

19.8 Each individual is responsible for keeping their own password secure and ensuring that it is neither disclosed to, nor used by anyone else under any circumstances.

19.9 The CCG does not currently allow users to store passwords or use password management software.

19.10 Staff are accountable for the security of their password and other identity tokens. This includes but is not limited to their:

- network login;
- encryption password for laptop;
- RSA token;
- Smartcard PIN;
- any digital certificate that uniquely identifies them.

19.11 If staff believe that any of their credentials have been compromised, they must immediately change the password, where possible, and log an incident via the IT service desk. This incident will then be investigated to establish the root cause of the breach.

19.12 Staff remain accountable for all activity undertaken using their identity on any system and, wherever possible, this activity is monitored for misuse.

Network Access

19.13 The CCG conforms to the NHS.net Code of Connection and as far as practical applies the good practice guidelines contained in the following guidance: http://systems.digital.nhs.uk/infogov/security/infrasec/gpg

19.14 All devices connected to the CCG network must be authorised by the IM&T team, the Information Security Manager or the DSPAT and meet all required standards.

Anti-Virus/Anti-Malware

19.15 Precautions must be taken to prevent and detect computer viruses and malware. Information Management and Technology (IM&T) manages antivirus software and will provide advice and support on virus control.

19.16 Individual Staff members are responsible for ensuring that the Antivirus is running on their laptop/Desktop. IT can provide guidance on how to do this.

19.17 Staff must contact the IT Service desk immediately if they receive a notification that a virus or any other form of malware has been detected on their device.eg Pop up/email/phone call

Secure Transmission of Confidential Information

19.18 All confidential, sensitive or person identifiable information must be transmitted securely in accordance with the Guidance on the Secure Transmission of Information which is available on the intranet, and the Confidentiality: Staff Code of Conduct which is issued to all staff at induction.

19.19 Where it is not possible to transmit confidential information in accordance with the requirements set out in the Guidance, a risk assessment must be carried out and approved by the DPO.

Access to email or documents

19.20 There may be occasions when it is necessary to access email messages from an individual's mailbox or documents when a person is away from the office for a length of time. Where it is not possible to contact the member of staff to gain permission, authorisation will be requested from the SIRO or DPO and access will then be granted in accordance with CCG approved process.

Email Services

19.21 There are types of email that are expressly prohibited and could result in formal disciplinary proceedings or be used as evidence in legal proceedings. These include, but are not limited to, sending:

- emails containing derogatory, libellous, defamatory, offensive, harassing, racist, obscene or pornographic remarks or depictions;
- comments which are not permitted in the spoken or paper environments;
- confidential messages without the express permission of the sender;
- messages from another employee's account;
- chain letters, junk letters, jokes or unsolicited email messages.

19.22 All communications are subject to Data Protection and Freedom of Information legislation and can also form part of the corporate record. Staff should also be aware that email messages could be used as evidence in legal proceedings.

19.23 Communications containing inaccurate information in the form of opinion or fact about an individual or organisation may result in legal action being taken against the person sending the email message and anyone forwarding the email message on to others.

19.24 Limited personal use of the CCG email system and internet access is allowed. However, the transmission of work data across personal email and messaging systems is strictly prohibited.

19.25 To protect the network, all emails are monitored for viruses. All email traffic (incoming and outgoing) is logged automatically. The logs may include email content.

19.26 The content of emails is routinely monitored for security purposes (e.g. malware, phishing, spam).

19.27 Staff are not permitted to use CCG devices or systems for any private commercial purpose.

19.28 The use of the CCG email address to register on internet websites for non-CCG purposes is not permitted. This is to reduce the risk and incidence of cyber-crime activity.

Pseudonymisation and Safe Havens

19.29 The CCG occasionally uses patient identifiable information for purposes other than healthcare; this is known as secondary use. It is NHS policy and a legal requirement that when patient data is used for purposes not involving the direct care of the patient, the patient should not be identified unless it can be done so legally. The NHS Confidentiality Code of Practice states the need to 'effectively anonymise' patient data prior to any non-direct care use.

19.30 Data cannot be labelled as primary or secondary use data; it is the purpose of the disclosure and the usage of the data that is either primary or secondary. This means that it is legitimate to hold data in an identifiable form, but it becomes essential to ensure that only authorised users are able to have identifiable data disclosed to them.

19.31 All NHS organisations require safe haven processes to maintain the privacy and confidentiality of the personal information held by the organisation. The implementation of these processes facilitates compliance with the legal requirements placed upon the organisation, especially concerning sensitive personal and confidential information.

19.32 Additionally, employees of the CCG, when disclosing information to other organisations both within and outside the NHS, must seek an assurance that suitable processes are in place to receive confidential information in a way that ensures the security, integrity and confidentiality of that data.

19.33 The NHS Code of Practice: Confidentiality requires that the use of patient data for purposes not directly contributing to the safe care of the individual concerned must be 'effectively anonymised' (in a de-identified form).

19.34 To ensure that the CCG is able to maintain systems and support for the delivery of healthcare services, the organisation has attained **Accredited Safe Haven Status (ASH)**. This means that where person confidential data is received / sent for secondary purposes, New Safe Havens are in place to restrict access and support the pseudonymisation process.

Smartcards

19.35 CCG users of Smartcards must follow the terms and conditions of use listed on the Spine Portal: https://portal.national.ncrs.nhs.uk/portal/dt Smartcards should be treated with care and protected to prevent loss or damage.

Internet Use

19.36 The CCG has developed an Internet Acceptable Use Policy to control internet usage across the CCG. This can be found on the CCG intranet.

Security of Assets

19.37 All major information assets have a nominated owner (IAO) who is responsible for security measures and for the detailed risk assessment for each asset. These are included in the Information Asset Register and are reviewed on a regular basis.

19.38 IAOs will audit information and cyber security arrangements and monitor access to any confidential information held on the Information Assets.

Remote or Off-Site Working

19.39 Remote or off-site working must be approved by line managers, and staff must refer to the Remote Access and Off-Site Working Policy.

System Back-ups

19.40 Computer system back up recovery points are at the following intervals:

- 8.00am;
- 12.00 midday;
- 8.00pm.

19.41 Following the total catastrophic loss of the site, the recovery point would be up to one week.

Privacy by Design and by Default - Systems Development, Planning and Procurement

19.42 Security issues must be considered and documented during the requirements phase and the procurement phase of all system procurements and developments – this is known as Privacy by Design and by Default. A DPIA must be completed and minimum security standards must be incorporated in all new systems.

19.43 New operational software must be quality assured. System test and live data should be separated and adequately protected. All changes to the systems, including externally commissioned systems, must pass through a formal change control procedure.

Business Continuity Planning and Disaster Recovery

19.44 The CCG has processes in place to maintain appropriate plans for the restoration of all critical IT systems. The CCG plans to recover all systems by day three following total catastrophic loss of all systems on a site. There is an order of recovery of the systems in place.

19.45 All systems will have threats and vulnerabilities assessed to determine how critical they are to the CCG. Individual work areas have procedures in place to maintain essential services in the event of IT system failure.

19.46 Disaster Recovery and Business Continuity Plans are in place for the CCG and cover areas such as back-up, media control, event logging, monitoring, protection from theft and damage, unauthorised access and capacity planning. The disaster recovery plans are tested on an annual basis.

20. CLOSED CIRCUIT TELEVISION (CCTV)

20.1 CCTV is in operation at the entrances to Canford House and Vespasian House in order to monitor the security of the buildings. The CCTV is operated and managed by the Discovery Court Business Centre at Canford House, and RTI Estates Ltd. at Vespasian House.

20.2 Further information on the use of CCTV is set out in the Building Operational Handbook, which is available on the CCG intranet. Any requests for information about the CCTV, or any subject access requests should be directed to the above organisations.

21. STRATEGY

21.1 The CCG aims to achieve a standard of excellence in DSP by ensuring that information is dealt with legally and securely during the course of CCG business, in order to support high quality patient care.

21.2 The CCG aims to minimise and manage the key risks arising from information handling processes. These are:

- legal action due to non-compliance with statutory and regulatory requirements;
- loss of public confidence in the CCG;
- contribution to clinical or corporate negligence.

21.3 The CCG will ensure that the work necessary to implement the standards required for DSP will be carried out through an annual DSP Implementation Plan arising from a baseline assessment against the standards set out in the DSPT. Regular reports relating to DSP progress will be submitted to the IAOG which in turn will report to the Audit Committee.

21.4 The CCG will also ensure that detailed policies and procedures for DSP are available to all staff, with the Confidentiality: Staff Code of Conduct booklet acting as a staff guidebook for all issues.

21.5 The IAOG will further ensure the embedding of DSP across the organisation through training. As information plays a key part in all corporate and clinical activities, training appropriate to the needs of individuals and staff groups will be delivered, using the most appropriate mechanism set out below.

22. TRAINING

22.1 It is recognised that the successful implementation of DSP Policy is dependent upon the input and commitment of staff at all levels of the organisation.

Induction

22.2 New staff will receive a DSP induction, delivered by the DSPAT, as part of their corporate induction. They will also be issued with a copy of the booklet 'Confidentiality: Staff Code of Conduct' at their induction. IT equipment will only be issued upon receipt of confirmation that Induction training has been booked.

Annual Training

22.3 Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. All staff including contractors, temporary staff, and students are required to attend mandatory annual data security and protection training which is run by the DSPAT and tailored to individual staff groups.

22.4 Subsequent training needs for individual staff members will be identified through the appraisal process/individual performance review process.

22.5 The DSPAT, as required, will provide additional ad hoc DSP training, for example, following an incident relating to a personal data breach.

22.6 Specific staff roles have also been identified to receive additional training and these are set out in the DSP Training Plan and Training Needs Analysis at **Appendix C**.

22.7 The Workforce Directorate and the DSPAT will monitor take up of the training and report to the IAOG. Where there is a low take-up of training, this will be reported to Directors for action.

23. CONSULTATION

23.1 This policy is a legislative requirement and no consultation is required.

24. RECOMMENDATION AND APPROVAL PROCESS

24.1 Refer to Section C – Document Details at the front of this policy.

25. COMMUNICATION/DISSEMINATION

25.1 Refer to Section G – Distribution List at the front of this policy.

26. IMPLEMENTATION

26.1 This policy does not require any new aspects to be implemented.

26.2 This policy will be made available to staff through the intranet as detailed in the CCG's Policy for the Management of Procedural Documents.

27. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE DOCUMENT

27.1 The IAOG takes overall responsibility for ensuring compliance with the policies and procedures summarised in this policy, reporting to the SIRO and the Caldicott Guardian who ensure Governing Body level assurance.

27.2 Year on year improvement within the DSP agenda will be monitored through the DSPT, which is submitted to NHS Digital on an annual basis.

27.3 Minutes from the IAOG are submitted to the Audit Committee. Following each IAOG meeting, a report summarising the issues discussed at the meeting is prepared and issued to the Audit Committee and the Directors Performance Group. An annual report is also provided to the Governing Body, together with the scores of the DSP Toolkit assessment.

27.4 The annual work plan for DSP will be reviewed and monitored by the IAO Group to provide assurance on the level and suitability of the evidence to support the DSP Toolkit self-assessment scores.

27.5 Additionally, the DSPAT will carry out compliance audits to monitor compliance with this policy. Any actions as a result of these audits will be monitored by the IAO Group.

27.6 Compliance with this policy will also be measured against the criteria for Record Keeping in relation to the National Health Service Litigation Authority.

28. DOCUMENT REVIEW FREQUENCY AND VERSION CONTROL

28.1 This policy 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 or the Information Commissioner.

28.2 Any changes made throughout the year will be issued as amendments to the framework. Such amendments will be clearly identifiable to the section to which they refer and the date issued. These will be clearly communicated via the CCG weekly bulletin.

APPENDIX A

GLOSSARY

Phrase	Definition
Personal Data	The provisions of the DPA apply only to personal data. The term 'personal data' is defined, in Article 4 of the GDPR as "*any information relating to an identified or identifiable person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*
Special Category Data	Data defined in Article 9 of the GDPR as "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".*
Subject Access Request (SAR)	Subject Access Rights give individuals the right to make an application in writing to gain access to information held, or processed, about them.
Data Controller	A 'data controller' is a person who (either alone or jointly or in common with other persons) determines the purposes for which, and the manner in which, any personal data is processed.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Subject	A 'data subject' means an individual who is the subject of personal data and must be a living individual. Provided that the data controller is subject to the Act, rights with regards to personal data are available to every data subject regardless of nationality or residence.
Information Commissioner	The Information Commissioner is responsible for administering the DPA and enforcing its provisions through powers vested in him and through the courts. Further information is available at www.ico.gov.uk.

Phrase	Definition
Record	Recorded information in any format of any type, in any location, which is created, received or maintained by the CCG in the transaction of its activities or the conduct of its affairs and is kept as evidence of such activity.
NHS Record	An NHS record is anything which contains information, in any media, which has been created or gathered as a result of any aspect of the work of the NHS employees, including agency, temporary, students or bank staff.
Corporate Record	A record that relates to an organisation's business activities, processes, activities and transactions.
Document	Not all documents are records. If for example, an email is sent asking the time of a meeting or forwarding a piece of information that is already in the public domain, the email is a document not a record. If, however, the email adds a new piece of information, supplies an appraisal on a member of staff or contributes to decision-making, then it becomes a record, because it is the only evidence of an action or activity.
Records Management	Records management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record.
Records Life Cycle	This term describes the life of a record from its creation/receipt through the period of its active use, then into a period of inactive retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.
Data Quality	Data quality is the ability to supply accurate, timely and complete data, which can be translated into information whenever and wherever, required. Data quality is vital to effective decision making at all levels of the organisation.
Safe Haven	Safe Haven is a term used to encompass all processes and procedures put in place to ensure that confidential information is protected from loss, damage or unauthorised access at the time it is received.

Phrase	Definition
Pseudonymisation	Pseudonymisation is a method which disguises the identity of patients by creating a pseudonym for each identifiable patient data item. This allows patient linking analysis which is required within secondary uses.
Personal Identifiable Data (PID)	Personal identifiable data refers to any data, or combination of data, that can be used to identify an individual.
Primary Uses	Primary uses relates to information which is used for health care and medical purposes which directly contributes to the treatment, diagnosis or the care of the individual and includes relevant supporting administrative processes.
Secondary Use Service	The Secondary Use Service (SUS) is primarily a data warehouse which provides access to anonymous patient-based data for purposes other than direct clinical care. SUS is delivered by the NHS Information Centre and NHS Connecting for Health.
BYOD (Bring your own device)	BYOD is the use of employee-owned devices for business purposes within an organisation.

APPENDIX B

TERMS OF REFERENCE

Information Asset Owners Group

1. AUTHORITY AND PURPOSE

1.1 The key authority and purpose of the Group is to:

- ensure that the NHS Dorset Clinical Commissioning Group (CCG) has effective policies and management arrangements covering all aspects of data security and protection (DSP) in line with the CCG's Data Security and Protection Policy, including maintaining the currency of the policy and other associated policies, strategies, guidance and procedures in accordance with national standards;

- to advise the Governing Body on issues relating to DSP and include those specific to:

  - provision of information services;
  - management of records;
  - Data Protection Act 2018;
  - EU General Data Protection Regulation 2016;
  - confidentiality;
  - sharing of information;
  - Freedom of Information Act 2000;
  - Human Rights Act 1998;
  - Access to Medical Reports Act 2009;
  - cyber security;
  - legal basis of data flows;
  - information risk.

- agree, and sign off (as delegated by the Governing Body), the appropriate components of the DSP Toolkit Assessment;

- develop the CCG's DSP work programme and monitor progress of the work;

- ensure the CCG's approach to data security, information handling, and respecting the confidentiality of service users, is communicated to all staff and made available to the public;

- offer support, advice and guidance to the Caldicott Guardian, the Senior Information Risk Owner (SIRO) and the Data Security and Protection programme within the CCG;

- review and discussion of incident reports into personal data breaches, undertaking investigation and providing recommendations for remedial action, where appropriate;

- review Data Protection Impact Assessments (DPIA) for new projects and maintain an overview of the robustness of the DPIA process across the organisation;

- review and monitor the organisational information asset register and supporting documentation and risk assessments;

- review and monitor flows of information in and out of the organisation, including the legal basis for these flows;

- work with the CCG to ensure records are managed in an appropriate way and in accordance with GDPR;

- support DSP within the contracting and procurement process;

- ensure that mandatory DSP training made available by the CCG is taken up by staff on an annual basis as necessary to support their role, and monitor attendance levels across the organisation;

- promote sound DSP principles across the CCG with key stakeholders, including staff and independent NHS contractor professions and ensure staff have access to appropriate and up to date guidance;

- liaise with other healthcare trusts, organisations, committees and working groups in order to promote Information Governance issues;

- review and approve all information sharing agreements for the CCG.

2. MEMBERSHIP

2.1 Information Asset Owner Definition

2.2 Must be senior/responsible individuals involved in running the CCGs business. Their role is to understand what information in held, what is added and what is removed, how information is moved and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and the use of their asset annually to support the audit process.

2.3 The IAO Group membership comprises members with sufficient authority to ensure the DSP work programme is understood and where necessary completed by directorates. Alongside the nominated IAOs, membership will include the following members:

- Caldicott Guardian;

- Senior Information Risk Owner;

- Data Protection Officer;

- Data Security Officer;

- Workforce Lead;

2.4 The group will be chaired by the Senior Information Risk Owner.

2.5 The Group may co-opt other members from time to time as relevant to the business being considered.

3. ATTENDANCE, FREQUENCY, LOCATION AND TIMING OF MEETINGS

3.1 The IAOG will meet quarterly. Meetings will be held at Vespasian House or Canford House.

3.2 All members of the group are required to attend meetings or provide appropriate and informed representation in their absence for continuity purposes.

3.3 All members of the group are required to provide brief progress reports on their specific areas of work and bring pieces of work to the group for discussion and approval, where relevant.

3.4 Other representatives who are not members of the Group may be invited to attend for all or part of a discussion, particularly when the Group is discussing areas of operation that are the responsibility of that representative.

3.5 The Group can also invite representatives of partner and stakeholder organisations to attend meetings on an ad hoc or routine basis.

3.6 In order to fulfil its remit, the IAOG may obtain any professional advice it requires and invite, if necessary, external experts.

3.7 The DSPAT will be responsible for the administration of the IAOG and the timely production of the minutes.

4. REPORTING

4.1 Formal minutes will be kept of the meetings and submitted for approval at the next meeting.

4.2 The draft minutes will be cleared by the Chair of the IAOG and / or a nominated lead.

4.3 Unless papers or items are marked as ‘restricted’, then members of the IAOG will be expected to share the information with their colleagues.

4.4 Overarching reports from the IAOG will be taken to the Governing Body via the Audit Committee.

4.5 Prior to submission to NHS Digital, the IAOG will agree the annual DSP Toolkit Assessment report.

5. AUTHORITY

5.1 The IAOG is authorised by the Governing Body to investigate any activity within its terms of reference. The Group is authorised to seek any information

it requires from any employee, and all employees are directed to co-operate with any request made by the Group.

5.2 The Group is also authorised to implement any activity which is in line with the terms of reference, as part of the DSP work programme.

6. APPROVAL OF TERMS OF REFERENCE

6.1 These terms of reference were approved by the IAOG on 27 March 2020.

6.2 The terms of reference will be reviewed on an annual basis by the IAOG.

APPENDIX C

DATA SECURITY AND PROTECTION TRAINING PLAN AND TRAINING NEEDS ANALYSIS

1. INTRODUCTION

1.1 To ensure organisational compliance with the law and central guidelines relating to Data Security and Protection (DSP), DSP training is considered to be 'Core' mandatory training that **all** staff within the NHS Dorset Clinical Commissioning Group (CCG) are required to complete within two weeks of commencing employment, and thereafter on an annual basis at the relevant directorate training sessions. IT equipment will not be issued until Induction training has been booked.

1.2 To meet this requirement, the CCG has established a clear plan for DSP training that is appropriately tailored to specific staff groups or job roles. This plan addresses how and when each work area and/or staff group will be trained, how training needs beyond the basic level will be addressed, and also includes induction processes for new staff.

2. DSP TRAINING OVERVIEW

2.1 The NHS Operating Framework – 'Informatics Planning 2010/11' provides guidance on the informatics components of local operating plans, and national expectations for the NHS for delivery of national and local objectives are set out. Under 'Annex 1 National Expectations' the section on sustaining robust information governance states that:

'All staff should receive annual basic IG training appropriate to their role through the online NHS IG Training Tool'

2.2 The 'Information Governance Review - Information: To Share or Not to Share?' which was carried out by Dame Fiona Caldicott and published in March 2013. The report highlighted that:

- "… mandatory training is often a 'tick-box exercise'. Although mandatory training such as the online NHS Information Governance Training Tool may provide an introduction to some information governance issues, this 'one size fits all' approach is too often focused on processes and policies in organisations… In fact, it is possible to pass the training tool by answering the questions at the end without bothering to read the text."

2.3 One of the recommendations of this report is that there is:

- "… a fundamental cultural shift in the approach to learning about information governance across health and social care…".

2.4 With this in mind, staff groups will be required to attend mandatory annual DSP training, run by the DPO, and tailored to individual staff groups.

3. TRAINING NEEDS ANALYSIS

3.1 Staff will inevitably have different levels of awareness of their responsibilities for safeguarding confidentiality, protecting information and preserving information security. Whilst the mandatory basic DSP training will be sufficient to give staff the knowledge they require, some jobs will require additional training and some staff may require additional support.

3.2 This will be addressed by regular assessment of training and development needs, consideration of how these needs might best be met and evaluation of any training that has been undertaken.

3.3 All staff will receive an annual appraisal and a mid-year review which will set out the skills and competencies required to perform a particular job role and then an assessment of the current level of skills and competencies of the staff member performing the job. Where a skills/competency gap is identified, appropriate training will then be arranged.

3.4 Skills/competency gaps will be analysed to see if there is a common theme in each area of the organisation where additional training programmes can be planned for the future.

Staff Induction

3.5 Staff induction for all new starters needs to ensure that DSP training needs are addressed. New members of staff may otherwise fail to be aware of the relevant requirements and guidelines about their own individual responsibilities for DSP compliance.

3.6 Therefore, all new starters will receive face-to-face DSP training within two weeks of commencing employment, delivered by the DSPAT, as part of their corporate induction. They will also be issued with a copy of the booklet 'Confidentiality: Staff Code of Conduct' at their induction. IT equipment will only be issued upon confirmation that Induction training is booked.

3.7 DSP induction training will be tailored to an individual's role, covering:

- introduction to DSP in the CCG working environment;
- fundamentals of the Data Protection Act 2018 and the Caldicott Principles;
- Freedom of Information Act 2000 and individual responsibilities;
- NHS Constitution;
- basic information security and records management guidance;
- pointers to where policies, procedures and further information are located.

3.7 Once induction has been completed, new starters will be required to attend their directorate facilitated training session during the course of the year or within 3 months of commencing employment.

Annual DSP Training

3.8 Existing staff will be required to attend mandatory annual DSP training sessions which will be run by the DPO. The training will cover key areas such as information security, records management, Freedom of Information Act 2000, Data Protection Act 2018, NHS Constitution, Caldicott Principles and updates on any recent monetary penalties issued by the Information Commissioner's Office or any changes to guidance and legislation. The training will be tailored to the needs of individual staff groups and several sessions will be run for each directorate. All staff will be expected to attend one of these sessions.

3.9 The areas covered by the training will be reviewed and updated on an annual basis, following an evaluation of staff competence during the training sessions and the outcome of DSP staff compliance audits. Organisational and legislative requirements will also be taken into consideration.

3.10 Subsequent training needs for individual staff members will be identified through the appraisal process/individual performance review process.

3.11 Additional ad hoc information governance training will be provided by the DSPAT as required, for example, following an incident relating to a confidentiality breach.

3.12 Specific staff roles have also been identified to receive additional training, for example, IAO Group members will receive additional DSP training to enable them to carry out their roles in providing data security and protection and support to their directorates.

Data Security and Protection Team

3.13 The DSPAT will attend specialised Data Protection training which will be sourced according to the needs of the organisation. Not all members of the team will attend the same training; this will be dependent on work areas and team requirements.

IAOs

3.14 The IAOs will require additional data protection training to enable them to carry out their roles as the directorate specialists on Data Security and Protection. Specific training will cover the Data Protection Act in greater depth to enable the Leads to handle day-to-day issues. This training will be either delivered by the DPO, or sourced by an external provider.

Caldicott Guardian

3.15 The Caldicott Guardian is a specialist role requiring a detailed knowledge on confidentiality issues to enable the role to be performed effectively. To fulfil

this requirement, any newly appointed Caldicott Guardian will receive specialised training from an external provider in the first instance. This will then be updated through attendance at the CCG facilitated DSP training sessions, with occasional updates delivered by an external provider.

Senior Information Risk Owner / Information Asset Owners

3.16 The DSP Toolkit states that the SIRO should receive strategic information risk management training on an annual basis. To fulfil this requirement, any newly appointed SIRO will receive specialised training from external provider, followed by attendance at the CCG facilitated DSP training sessions on an annual basis, with occasional updates delivered by an external provider.

3.17 IAOs are required to have a good knowledge of risk management and business continuity arrangements for their key information assets. With this in mind, the IAO's will attend the facilitated DSP training sessions delivered by the DPO, and additional training will be provided on an individual basis around the risk assessment process for information assets.

Information Security Manager

3.18 The Information Security Manager is a specialist role requiring specific knowledge on Information Security Management and ISO 27001. To fulfil this requirement, any newly appointed Information Security Manager will receive specialised training from an external provider, followed by attendance at the CCG facilitated DSP training sessions on an annual basis, with occasional updates delivered by an external provider.

Staff handling Subject Access Requests

3.19 Staff handling subject access requests form part of the DSPAT, and as such, will receive specialised training as part of their annual training requirements. This will include training on accessing health records.

CCG Governing Body

3.20 The CCG Governing Body will receive specific training delivered by the DPO. This will largely focus on the corporate responsibilities of the Governing Body.

4. TRAINING MONITORING AND REVIEW

4.1 Training attendance will be monitored and recorded via the Electronic Staff Record (ESR), and the DSPAT will oversee take up of the training and report to the IAO Group. DSP training is mandatory for all staff and a 95% take-up is necessary to comply with the requirements of the DSP Toolkit.

4.2 Staff will be required to undertake a written paper to confirm knowledge following annual DSP training.

4.3 In addition, IAOs will provide regular reports on the progress of staff training uptake in their directorates to enable monitoring and chasing.

4.4 This training plan will be updated in line with any legal requirements, corporate and/or Department of Health policy, or any major changes which may impact on the DSP agenda, at a local or national level.