NHS
Dorset
Clinical Commissioning Group

NHS Dorset Clinical Commissioning Group

Data Protection Policy



Supporting people in Dorset to lead healthier lives

PREFACE

This document sets the policy for NHS Dorset Clinical Commissioning Group with regard to its legal obligation to comply with the Data Protection Act 2018.

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 is 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 for NHS Dorset Clinical Commissioning Group with regard to its legal obligation to comply with the Data Protection Act 2018.	

B	ASSOCIATED DOCUMENTS

- Data Security and Protection Policy
- Confidentiality: Staff Code of Conduct
- Confidential Corporate Information Policy
- Procedure for the Management of Adverse Incidents
- Procedure for the Management of Serious Incidents
- Remote Access and Off-site Working Policy
- Network Security Policy
- Freedom of Information Policy

C	DOCUMENT DETAILS
Procedural Document Number	14
Author	Paddy Baker
Job Title	Data Protection Officer
Directorate	Finance
Recommending committee or group	Data Security and Protection Group
Approving committee or group	Data Security and Protection Group
Date of recommendation (version 1)	March 2016
Date of approval (version 1)	15 March 2016
Version	1.4
Sponsor	Chief Finance Officer (SIRO)
Recommendation date	October 2020
Approval date	17 November 2020
Review frequency	Bi-annually

Review date	October 2022

D	**CONSULTATION PROCESS**		
Version No	**Review Date**	**Author and Job Title**	**Level of Consultation**
1.2	018	Paddy Baker, Data Protection Officer	Data Security and Protection Group
1.4	October 2020	Paddy Baker, Data Protection Officer	IAO Policy Review Sub Group

E	**VERSION CONTROL**				
Date of issue	**Version No**	**Date of next review**	**Nature of change**	**Approval date**	**Approval committee/ group**
March 2016	1.2	March 2018	This policy replaces the CCG Data Protection and Confidentiality Policy	15 March 2016	Data Security and Protection Group
August 2019	1.3	August 2020	Update of contact details	-	-
October 2020	1.4	October 2022	Updated to incorporate change from DSPG to IAOG, include breach reporting and further minor amendments	17 November 2020	IAO Policy Review Sub Group

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

F	SUPPORTING DOCUMENTS/EVIDENCE BASED REFERENCES	
Evidence	**Hyperlink (if available)**	**Date**
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
Data Protection Act	www.opsi.gov.uk	2018
General Data Protection Regulation		2016
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
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	DISTIBUTION LIST		
Internal CCG Intranet	**CCG Internet Website**	**Communications Bulletin**	**External stakeholders**
✓	✓	✓	Tick as appropriate

1. RELEVANT TO

1.1 This policy is relevant to all staff:

- within NHS Dorset Clinical Commissioning Group (hereafter known as the CCG) whether operating directly or providing services under a service level agreement or joint agreement;

- 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.

1.2 Failure to adhere to this policy, and its associated procedures, may result in disciplinary action.

2. INTRODUCTION

2.1 This policy relates to the processing of personal information and to the management of personal data about members of the public/patients/service users and staff.

2.2 The CCG is required by law to comply with the Data Protection Act 2018 (DPA), which is concerned with the lawful processing of information relating to an identified or identifiable natural person. To comply with the law staff, and/or others, who process personal information must ensure they follow the Data Protection Principles and the Caldicott Principles.

2.3 Personal data means any information relating to an identified or identifiable natural person. 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.

2.4 Like all NHS Organisations, the CCG holds and processes information about its employees, members of the public, patients and other individuals for various purposes (e.g. the effective provision of healthcare services, Continuing Healthcare or; for administrative purposes). To comply with the DPA, personal identifiable information must be collected and used fairly, stored safely and not disclosed to unauthorised persons.

2.5 The DPA applies to both manual and electronic data and lists the following as potential identifiers: a person's name, an identification number (e.g. a patient number or a national insurance number), location data (e.g. a GPS location reference from a person's mobile telephone) an online identifier (e.g. an individual's identity as used on social media, or an e-mail address). Biometric and genetic data are also covered.

2.6 For the purposes of the DPA, the CCG acts as the data controller for personal and special category personal data. A data controller is an organisation who determines the purposes for which, and the manner in which, personal data is

to be processed. Such processing may be carried out jointly or in common with other organisations.

2.7 The CCG must be able to demonstrate compliance with the six principles of the Data Protection Act 2018 when collecting, processing, and retaining personal data.

2.8 All of the principles should be observed in relation to *all* aspects of personal data processing unless an exemption applies.

2.9 The CCG has a legal obligation to comply with all appropriate legislation in respect of data and information security. It also has a duty to comply with guidance issued by the Department of Health and Social Care (DHSC), the Information Commissioner (ICO), other advisory groups to the NHS and guidance issued by professional bodies.

2.10 Compliance with the policy will provide assurance to the CCG, and to individuals, that all personal and special category personal data processed by the CCG is dealt with legally, securely and efficiently, in order to deliver the best possible care to patients.

2.11 The CCG will establish and maintain policies and procedures to ensure compliance with the requirements contained in NHS Digital's Data Security and Protection Toolkit (DSPT).

3. SCOPE

3.1 To ensure that the CCG meets its legal requirements under the DPA this Policy applies to all staff within the CCG, Governing Body and Lay Members. It also applies to other personnel working for, and on behalf of, the CCG including agency staff, volunteers, students and contractors, third party partner organisations and suppliers.

3.2 This policy covers all:

a. data held and processed by the CCG in any medium;

b. information within the organisation, including (but not limited to):

- general public/patient/staff/service user information;
- personal information;
- special category personal data;
- organisational information.

c. aspects of handling information, including (but not limited to):

- structured and unstructured record systems – paper and electronic;

- transmission of information – post, telephone and electronic communications means;
- information systems managed and/or developed by, or used by the CCG;
- information sharing;
- tapes and other data from CCTV Systems;
- data held in offsite archive storage;
- data held on digital memory devices, laptops, tablets and any other type of mobile media.

4. PURPOSE

4.1 The purpose of this policy is to ensure that the CCG is compliant with the requirements of the DPA.

4.2 The CCG recognises its responsibilities to implement, in full, its duties in respect of the DPA and to ensure all its employees understand and implement the requirements.

4.3 This policy will underpin any operational procedures and activities connected with the implementation of the DPA, in particular those listed in the CCGs Data Security and Protection Policy.

5. DEFINITIONS

See Glossary at Appendix A.

6. ROLES AND RESPONSIBILITIES

CCG Governing Body

6.1 The CCG Governing Body supports the six Data Protection principles and the requirements of the Common Law Duty of Confidentiality and endorses this Data Protection Policy.

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

Chief Officer

6.3 The Chief Officer has overall responsibility for the Data Protection Policy within the CCG.

6.4 The Chief Officer is the named officer with responsibility for ensuring that the CCG complies with its statutory obligations and Department of Health and Social Care directives for Data Protection.

6.5 The Chief Officer will ensure that the CCG has access to specialist advice regarding the requirements of the DPA 2018. This will be provided by the CCG's Data Protection Officer in the first instance and then by the Information Commissioner's Office (ICO).

6.6 Responsibility for implementation of the DPA has been delegated to the Data Protection Officer.

Caldicott Guardian

6.7 The CCG has appointed a Caldicott Guardian, who oversees disclosures of patient information with particular attention being paid to those disclosures which are not routine.

6.8 The Caldicott Guardian ensures that the CCG and partner organisations protect the confidentiality of patient level information, and is responsible for advising the CCG and the Governing Body on confidentiality issues. This also includes establishing and maintaining procedures governing access to, and the use of, person confidential data held or processed within the CCG and the transfer of such data from the CCG to and from other bodies.

Senior Information Risk Owner

6.9 The Senior Information Risk Owner (SIRO) takes ownership of information risk and is responsible for:

- overseeing compliance with the Data Security and Protection Policy;
- ensuring the Governing Body is adequately briefed on information risk;
- reviewing and approving the information security risk assessments of CCG information assets;
- providing a focal point for the resolution and discussion of information risk issues.

Data Protection Officer

6.10 The Data Protection Officer will provide specialist advice on data protection to the CCG, along with the Data Security and Protection Team, working with the Information Asset Owners Group and the Caldicott Guardian.

6.11 The Data Protection Officer will also be responsible for:

- developing and maintaining policies, procedures and guidance as required by the DPA;

- maintaining and holding a record of the CCG's personal data held and the processing purposes under the DPA;

- periodically producing and distributing staff guides on Data Protection and Confidentiality;

- ensuring that all staff are aware of their personal responsibilities for compliance and adhere to organisational policies and procedures. This includes ensuring that training and written procedures are widely disseminated and available to all staff.

- dealing with subject access requests for the CCG;

- acting as an initial point of contact for any data protection and confidentiality issues which may arise and assisting with investigations into complaints about breaches of the Act;

- facilitating action in areas identified as non-compliant;

- co-ordinating the Data Security and Protection work programme and completion of the DSPT annual assessment.

Information Asset Owners Group

6.12 The CCG has established the Information Asset Owners Group (IAOG) comprising of all Information Asset Owners within the CCG in order to promote a consistent approach to Data Protection. The group is responsible for developing and sharing best practice across the organisation and ensuring that data protection standards are included in other work programmes and projects.

6.13 The key authority and purpose of the Information Asset Owners Group is to:

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

- offer support to, and ensure compliance with the Data Protection programmes within the CCG;

- ensure that the CCG has effective policies and management arrangements covering all aspects of confidentiality, data security and protection;

- review, approve and monitor Data Protection Impact Assessments to ensure privacy considerations are taken into account when new projects are introduced or changes are made to existing services;

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

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

Managers

6.15 The day to day responsibility for enforcing this policy will be delegated to Line Managers. Managers will ensure that all staff:

- are made aware of the data protection policy;
- attend appropriate training;
- know how to deal with requests for person identifiable information.

6.16 Managers will ensure that all systems and manual files that process personal data are recorded on the Information Asset Register and are managed by a nominated Information Asset Owner.

Information Asset Owners (IAOs)

6.17 The IAO must ensure that any system (and users) they are responsible for complies with the current Data Protection legislation.

6.18 The IAO is 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;
- expert advice is available regarding data protection issues;
- unusual requests for disclosure are scrutinised;
- within their area of control, all data flows in and out of the CCG containing personal identifiable information are recorded on the Record of Processing Activities;
- there is a system security procedure which outlines the media, frequency and retention period for back-ups of the data and programs for the system(s) within their control.

Director of Engagement and Development

6.19 The Director of Engagement and Development is responsible for overseeing all staff requests for access to personal files, with support from the Data Security and Protection Team.

6.20 The Director of Engagement and Development will ensure that appropriate clauses are in the terms and conditions of employment to ensure that all staff are bound by the requirements of the DPA.

Staff

6.21 All staff are expected to adhere to this policy and associated documentation. Any breaches of this policy will be investigated in line with the CCG disciplinary procedures.

6.22 All staff are required to attend data protection training on an annual basis, and any additional training as appropriate.

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

6.24 All staff who create, receive and use records have records management responsibilities. Staff:

- are responsible by law for any records they create and use;
- must be aware that any records they create are not their personal property, but belong to the CCG.

Information Commissioner's Office (ICO)

6.25 The ICO is the UK's independent public authority with responsibility to uphold information rights. They rule on complaints, provide information to individuals and organisations and take appropriate action when the law is broken.

6.26 The ICO is the national regulator of the following legislation:

- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Privacy and Electronic Communications Regulations 2003;
- Environmental Information Regulations 2004;
- INSPIRE Regulations 2009.

6.27 The ICO maintains a public register of data controllers who process personal information.

6.28 Where serious breaches of legislation occur, the ICO will consider whether an administrative fine is appropriate. Fines may be imposed on the controller and/or (in certain circumstances) any processors involved in a breach. The legislation sets the upper limits for fines and is split into two broad categories. Within the first category are the types of infringements that can result in a fine

of up to €10m, or 2% of worldwide annual turnover. The second category contains the types of infringement that can result in a fine of up to €20m, or 4% of worldwide annual turnover (whichever is higher).

7. SUPPORTING POLICIES AND PROCEDURES

7.1 A summary of CCG key policies and procedures that support the Data Protection work programme are listed at Section B of this document.

7.2 This is a live document and as new legislation, guidance and policies are approved, amendments will be added to this document.

8. THE DATA PROTECTION ACT

8.1 The Data Protection Act 2018 came into force on the 25 May 2018 and applies to all data relating to an identified or identifiable natural person (a living individual) held in manual files, computer databases, videos and other automated media. This includes personnel and payroll records, medical records, other manual files, microfiche/film etc.

8.2 The DPA requires the amount of data collected, and the access to it, to be minimised to that required to provide the service or perform the function. Print-outs and paper records must be treated carefully and disposed of in a secure manner, and staff must not disclose information outside their line of duty.

8.3 The DPA also requires the CCG to register with the ICO. The CCG will identify the purposes for holding the data, how it is used and to whom it may be disclosed on the CCG website. Failure to register or an incorrect registration is a criminal offence and may lead to the prosecution of the organisation.

8.4 Under a provision within the Data Protection Act, an individual can request access to their personal information regardless of the media in which this information may be held / retained. The CCG has a Subject Access Procedure for dealing with such requests (please refer to the Data Security and Protection Policy).

8.5 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. The CCG must comply with these principles.

Data Protection Principles

Principle 1

8.6 Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’).

Principle 2

8.7 Personal data shall be collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ('purpose limitation').

Principle 3

8.8 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').

Principle 4

8.9 Personal data processed shall be accurate and, where necessary, kept up to date ('accuracy').

Principle 5

8.10 Personal data shall be kept in a form which permits identification for data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').

Principle 6

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

For full overview of the data protection principles and their application see Appendix B.

9. CALDICOTT PRINCIPLES

9.1 Following a review of how confidential patient information was handled by the NHS, set out in the Caldicott report, the committee conducting the review recommended that each NHS organisation:

- identify a senior person as the Caldicott Guardian;
- implement seven principles (known as the Caldicott Principles) as good practice for all NHS organisations to adopt.

9.2 The Caldicott principles 'mirror' the requirements of the DPA 2018 and are good practice with which staff in the NHS are required to adhere.

9.3 For a full overview of the Caldicott principles and their application see Appendix C.

10. DATA SECURITY AND CONFIDENTIALITY

10.1 The CCG will ensure that personal data is held securely and adequately protected from loss or corruption and that no unauthorised disclosures of personal data are made.

10.2 All personal information relating to members of the public/patients/service users and staff must be kept secure at all times. The CCG has ensured there are adequate procedures in place to protect against unauthorised processing of information and against accidental loss, destruction and damage to this information. Please refer to the following guidance contained within the CCG's Data Security and Protection Policy:

- guidance for carrying out data protection impact assessments and the data protection impact assessment template;
- guidance on the introduction of bring your own device;
- guidance and procedure for managing subject access requests;
- guidance and procedure for the management of records;
- guidance on data quality;
- guidance on the secure transmission of information;
- guidance on pseudonymisation and safe havens;
- guidance on the secure use of smartcards.

11. INFORMATION SHARING

11.1 Whilst there is a public expectation of appropriate sharing of information between organisations providing health care services to them, and with other organisations providing related services, the public rightly expect that their personal data will be properly protected.

11.2 When sharing personal information, CCG staff must ensure that the Principles of the DPA 2018, the Human Rights Act 1998, the Caldicott Principles and the Common Law Duty of Confidentiality are upheld.

11.3 Information should only be shared for a specific lawful purpose or when appropriate consent has been obtained.

11.4 When identifiable information is to be used/shared for non-direct patient care the CCG must ensure that members of the public/patients/service users are aware of the use of the information and provide a means for the member of public/patient/service user to opt out.

11.5 The CCG has provided an information booklet and set out details on the CCG website informing members of the public/patients/service users why their information is collected, how it may be used and who it may be shared with. Staff must ensure that this information is provided to patients when their personal information is first collected.

11.6 Information sharing protocols (ISP) provide the basis for facilitating the exchange of information between organisations. Dorset CCG has a template

ISP for use by staff which is available from the Data Security and Protection Team (contact details in Appendix E).

11.7 All ISPs must be agreed by the IAO Policy Review Sub Group.

11.8 Some disclosures of information may occur because there is a statutory requirement upon the CCG to disclose e.g. with a Court Order, because other legislation requires disclosure such as tax office, pension agency (for staff), and notifiable diseases (for patients). See Appendix D for further information.

11.9 Before sharing information staff must:

- ensure there is a justifiable need to know;
- ensure there is a legal basis for sharing;
- anonymise/pseudonymise the data wherever possible;
- inform the member of public/patient/service user that basic information will be shared;
- seek the individual's consent to disclosure, as appropriate, in accordance with local protocols;
- keep disclosure to a minimum.

11.10 Please contact the Data Protection Officer for further advice relating to any form of disclosure of personal information. Contact details are available in Appendix E.

NHS Digital

11.11 Where data has been obtained from NHS Digital via a Data Service for Commissioners Regional Office (DSCRO) advice must be sought from them prior to release to ensure compliance with the terms of any Data Sharing Contract that may be in force.

Media

11.12 For all requests to share information relating to members of the public/patients/service users, staff must contact the Communications Team.

12. DATA PROTECTION CONTRACTUAL CLAUSES

12.1 The CCG is responsible for obtaining appropriate contractual assurance in respect of compliance with the DPA from all bodies that:

- have access to the CCG's information;
- conduct any form of information processing on its behalf.

12.2 This is particularly important where the information is about identifiable individuals as this is a legal requirement under the DPA.

13. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

13.1 The Information Commissioner's Office considers the use of a DPIA to be best practice and the CCG requires a DPIA to be completed at the beginning of any new project/service (or changes to services).

13.2 A DPIA helps assess and identify any privacy concerns, during a new project or change of service, enabling them to be addressed at the earliest opportunity.

13.3 The CCG has produced DPIA guidance to assist with the completion of DPIA's, and this can be found within the Data Security and Protection policy.

13.4 All DPIAs must be approved by the IAO DPIA Sub Group.

14. DATA BREACHES

14.1 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.

14.2 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.

14.3 Data breaches are discussed at the Data Security and Protection induction so that all staff are aware of their legal duty to keep strictly confidential any person identifiable data, commercially-sensitive and 'business in confidence' information that they are aware of (or associated with) during their employment and when they have left the CCG.

Data Breach Reporting

14.4 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.

14.5 Breaches are reported through the CCG data breach reporting system found on the Data Security and Protection Intranet page. High risk data breaches

are also reported via email to the Data Security and Protection Team to ensure action is taken within the statutory timeframe.

14.6 Reports of data breaches are provided to the IAO Group for review and discussion.

Mandatory Reporting of Data Breaches

14.7 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 individuals' rights and freedoms.

14.8 The ICO has asked all relevant health and social care organisations to use the incident reporting tool accessed via the Data Security and Protection Toolkit. 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.

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

Data Breach Investigations

14.10 Upon receipt of a data breach notification, a full investigation will be undertaken by a member of the Data Security and Protection Team.

14.11 A breach report will be produced and shared with the individual's line manager.

14.12 If an individual has three data breaches within a financial year, individual training will be provided by the Data Protection Officer and a letter will be sent to their line manager from the Data Protection Officer detailing further sanctions.

14.13 Continued breaches may result in disciplinary action.

15. COMPLAINTS

15.1 Any complaint which may be received because of a breach, or suspected breach, of the Data Protection Act 2018 will be dealt with under the CCG's Complaints Procedure and investigated by the DSP team.

16. TRAINING

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

Induction

16.2 New staff, including any staff working on secondment at the CCG will receive data security and protection training, delivered by the DSP team, as part of their corporate induction. They will also be issued with a copy of the booklet 'Confidentiality: Staff Code of Conduct' upon collection of their IT equipment.

Annual Training

16.3 Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. All staff are required to attend mandatory annual data security and protection training which is run by the DSP team and tailored to individual staff groups.

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

16.5 Additional ad hoc data security and protection training will be provided by the DSP team as required, for example following an incident relating to a confidentiality breach.

16.6 The Workforce Directorate and the DSP team 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.

17. CONSULTATION

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

18. RECOMMENDATION AND APPROVAL PROCESS

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

19. COMMUNICATION/DISSEMINATION

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

20. IMPLEMENTATION

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

20.2 This policy will be made available to staff through the intranet as detailed in the CCG's policy for the management of procedural documents.

21. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE DOCUMENT

21.1 The Information Asset Owners Group (IAOG) takes overall responsibility for ensuring compliance with this policy and any procedures relating to data security and protection contained within the CCG's Data Security and Protection Policy.

21.2 Following each IAOG meeting, any key issues or concerns will be escalated to the Audit Committee as part of the regular Data Security and Protection update. .

22. DOCUMENT REVIEW FREQUENCY AND VERSION CONTROL

22.1 This policy will be reviewed bi-annually or earlier if appropriate, to consider any changes to legislation that may occur, and/or guidance from the Information Commissioner.

Appendix A

GLOSSARY

Phrase	Definition
Corporate Record	Record that relates to an organisation's business activities, processes, activities and transactions.
Corporate and operational records held in any format by the CCG	Administrative records; staffing records; complaints records; financial and accounting records; photographs slides and other images (non-clinical); microform (microfiche and microfilm (non-clinical records); audio and video tapes, cassettes and CD-ROMs and DVDs; emails; computerized records (databases, output and disks); scanned documents; material intended for short term or transitory use including notes and spare copies of documents; diaries; any other material which holds non clinical information.
Data Controller	A 'data controller' is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
DPA	An acronym for Data Protection Act.
DSPT	The Data Security and Protection Toolkit.
Data Subject	A 'data subject' means the identified or identifiable living individual to whom personal data relates and must be a living individual. Organisations, such as companies and other corporate bodies of persons cannot, therefore, be data subjects. The 'data subject' need not be a United Kingdom national or resident. 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.
Disclosure	The divulging or provision of access to data.
Information Asset Owner (IAO)	An Information Asset Owner (IAO) will be a senior member of staff who is the nominated owner for one or more identified information assets of NHS Dorset CCG.
IAOG	Information Asset Owners' Group IAOG
Information Commissioner	The Information Commissioner is responsible for upholding the information rights for the UK public in the digital age as well as enforcing

	the law. Further information is available at www.ico.gov.uk.
Personal Data	The provisions of the DPA apply only to personal data. The term 'personal data' is defined, in section 4(1) of the Act as "*any information relating to an individual or identifiable natural person. 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".*
Personal Identifiable Data (PID)	Personal identifiable data refers to any data, or combination of data, that can be used to identify an individual.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Pseudonymisation	Means the processing of personal data so that the data can no longer be attributed to a specific data subject without the use of additional information, provided such additional information is kept separately and is subject to technical and organisational measures to ensure that the person is not identified or made identifiable.
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.
Special Category Personal Data	Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, physical or mental health condition, 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.
Third Party	Any person other than: • the data subject • the data controller

	• any data processor or other person authorised to process for the data controller.

Appendix B

Data Protection Principles

1. Principle 1 – personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

1.1 This requirement is concerned with making members of the public/patients/service users/staff aware of why the NHS needs information about them, how the information is used and to whom it may be disclosed. To comply, the CCG is required to produce patient and staff information leaflets to explain the use of information, and display details on the CCG website.

1.2 The CCG must ensure that the following information is made readily available:

- the identity and contact details of the data controller;
- the contact details of the Data Protection Officer;
- the purposes of the processing for which the data are intended;
- the legal basis for the processing (i.e. the lawfulness condition on which the data controller is relying);
- the recipients or categories of recipients of the data, if any;
- where applicable, the fact that the controller intends to transfer the personal data to a third country or international organisation.

1.3 The DPA makes specific provision for special category personal data. Any of the following data held by the CCG is considered to be 'sensitive' data within the DPA:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- physical or mental health;
- sexual orientation;

Article 6(1)

1.4 In order for processing of personal data to be lawful under data protection law, one of the following conditions must be met for each and every aspect of such processing:

- the data subject has given his or her consent to the processing of his or her data for one or more specified purposes;

- the processing is necessary:
  a) for the performance of a contract to which the data subject is a party, or;
  b) In order to take steps at the request of the data subject with a view to entering into a contract.

- the processing is necessary for compliance with any legal obligation to which the controller is subject;

- the processing is necessary to protect the vital interests of the data subject or another natural person;

- the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- the processing is necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties, except where such interests are overridden by the interests or fundamental freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

1.5 Conditions for processing special category personal data:

- explicit consent of the data subject;

- compliance with employment, social security, and social protection law obligations;

- vital interests of the data subject;

- processing by a not-for-profit body;

- personal data manifestly made public by the data subject;

- establishing, exercising, or defending legal claims or whenever courts are acting in their judicial capacity;

- substantial public interest;

- provision of medical or social care or treatment;

- public interest in the area of public health;

- archiving in the public interest, scientific or historical research, or statistical purposes.

1.6 When identifiable information is to be used for non-direct patient care the CCG must write to the patient/service user explaining the use of the information and provide a means for the patient/service user to opt out.

2. Principle 2 - personal data shall be collected only for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

2.1 Data can only be processed for the purpose or purposes for which it was originally obtained. When disclosing data, care must be taken to ensure that any person to whom it is disclosed is aware of the purpose or purposes for which the data was intended.

2.2 The Act requires that the CCG must specify the purpose of processing data (e.g. the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller i.e. for the provision and administration of Health Care), what data is to be included in this purpose, whom it will be disclosed to and if it is to be transferred overseas (see 1.2).

2.3 In doing so the CCG has to consider that data that it requires. The CCG is legally obliged to notify and register its collection purposes with the Information Commissioner. The current purposes that the CCG has notified are:

- Staff Administration;

- Accounts and Records;

- Health Administration and Services;

- Research;

- Crime Prevention and Prosecution of Offenders;

- Public Health;

- Data Matching.

2.4 Should any member of staff be processing personal data for any purpose other than those listed then you should immediately inform the Data Protection Officer.

3. Principle 3 – personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')

3.1 The Act requires that the CCG should only use the minimum amount of information required to fulfil the purpose. Staff should collect only data that is required for a specific purpose, and additional information should not be requested unnecessarily.

3.2 Furthermore, under principle 3, the controller should ensure access to personal data is limited for staff. Staff should only have access to the information they need to carry out their function.

4. Principle 4 – personal data processed shall be accurate and, where necessary, kept up to date ('accuracy')

4.1 The requirement to ensure that personal data are accurate is an absolute one. The DPA does not define accurate but the DPA 1998 gave a helpful definition of 'inaccurate': …data are inaccurate if they are incorrect or misleading as to any matter of fact.

4.2 The CCG must, therefore, take reasonable steps to ensure that all information held on any media, whether manual or electronic, is accurate and up to date. If data is out of date staff need to take steps to ensure accuracy before use.

4.3 Users of software will be responsible for the quality (i.e. accuracy, timeliness, completeness) of their data by carrying out their own quality assurance and participating as required in quality assurance processes.

4.4 Patient/service user and staff information held by the CCG should be checked on a regular basis for accuracy.

5. Principle 5 – personal data shall be kept in a form which permits identification for data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation')

5.1 The storage limitation principle requires the deletion, destruction, anonymisation, or pseudonymisation of personal data that are no longer needed for their purpose(s). There are no interpretive provisions in the Act that relate to this principle and there are no set time periods to which controllers must adhere. Thus, controllers will be required to make their own determinations as to an appropriate retention period having regard to the purposes for which the data were collected, and the information conveyed in the notice made available to data subjects.

5.2 This principle applies to all records, regardless of the media in which they are held, stored or retained. Staff should review all data regularly and archive information that is no longer required. The CCG has a Records Management Policy which follows the Records Retention Schedule documented in the Records Management NHS Code of Practice. The storing and destruction of all records should be in accordance with this policy and retention schedule.

5.3 A useful methodology for compliance is to draw up a 'data retention policy' or 'retention schedule' that sets out the relevant periods of time for which the data in relevant categories may be held.

5.4 Pseudonymisation is permitted as a method of complying with this principle

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

6.1 The aim of this principle is to ensure that appropriate care is taken of personal data, and that the attention of controllers and processors is focussed on this objective, with significant adverse consequences if they do not.

6.2 The consequences of a personal data breach are considerably more significant and require greater work on the part of the controller (and processor). In the case of serious breaches, organisations are required to inform both the ICO and all persons potentially affected.

6.3 When the CCG proposes to engage a processor to carry out data processing operations on its behalf, it must ensure that the processor provides sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the legislation.

Subject Access Requests (SAR)

Rights of access are conferred on data subjects to any information held relating to them unless certain very specific exemptions apply (e.g. the person is contemplating legal action against the organisation).

Individuals have the following rights:

- right of subject access:
    - individuals whose information is held by the organisation have rights of access to it; regardless of the media in which the information may be held/ retained. Individuals also have a right to complain if they believe that the CCG is not complying with the requirements of the Data Protection legislation;
    - the CCG must ensure an up to date procedure is in place to deal with requests for access to information. This can be found in the CCG Data Security and Protection Policy;
    - the Access to Health Records Act 1990 will remain to provide access rights to relatives, or those who may have a claim, to deceased patient's records;
    - once a request for information under the DPA has been received, no amendments or deletions to the data must be

made that would not have otherwise been made. In other words, the data must not be tampered with in order to make it acceptable;

- if information is requested that would reveal personal data other than the applicants, the third party must give consent before it can be released;

- solicitors and insurance companies may make requests on behalf of clients. The client involved **must** sign a written consent form, which needs to be received before any information is released.

- right to object to the processing of their data in a range of specified purposes e.g. direct marketing and to object to automated decision taking;

- right to take action for compensation if the individual suffers damage or distress;

- right to data portability;

- right to take action to rectify, block, erase or destroy inaccurate data;

- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

6.2 All patients / service users, or someone acting on their behalf, can request to have access to their information held by the CCG. All applications must be made in writing to the Data Security and Protection team. Please refer to the CCG Data Security and Protection Policy.

Appendix C

Caldicott Principles

1. **Justify the purpose(s)**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients (or staff) to be identified should be considered at each stage of satisfying the purpose(s).

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

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

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

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality.**
   Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix D

Disclosure of personal/sensitive information to the police and other agencies

1.1 It is sometimes necessary for external agencies to have access to personal information without the consent of the individual.

1.2 If there is a legal duty on the CCG and/or the applicant then disclosure is mandatory and consent is not necessary. This is often the case in the instance of Child Protection issues.

1.3 If the applicant has a legal power to request the information, you can disclose it, but it is not mandatory. This is often the case with police enquiries. The applicant must be able to demonstrate that consent would not be appropriate because of the nature of the investigation. In the instance of the police, this would be done under an exemption of the DPA 2018. A Schedule 2 (1)(a) exemption is used when making enquiries which are concerned with:

- the prevention and detection of crime; or
- the apprehension or prosecution of offenders.

1.4 This exemption allows information to be provided by organisations without gaining consent. However, you do not have to supply information, even though the Police have made a considered judgement about their need for information.

1.5 Do not feel pressurised to give information because the police have requested it. It is reasonable to ask why it is needed and what is required before making a decision.

1.6 Staff should always check the identity of anyone requesting information, and only the minimum information to satisfy the request should be given.

1.7 It is recommended that staff should seek advice from colleagues and line managers before making a decision about disclosure. The decisions made and any reasoning should be recorded, as a judgement may have to be made as to whether disclosing information would cause fewer problems than withholding it. Advice is available from the Data Protection Officer.

Disclosure under Legal Duty

1.8 The most likely legal basis for disclosure to the police is legal duty, where you MUST disclose, even without consent:

- **Prevention of Terrorism Act (1989) and Terrorism Act (2000)** – if you have gained information about a terrorist activity you MUST inform the police.
- **Court Order** – where the courts have made an order, you must disclose the required information, unless the organisation decides to challenge the order in court.

Disclosure under Legal Power

1.9 The other likely legal basis for disclosure to the police is legal power:

- **The Police and Criminal Evidence Act (1984)** – you can pass on information to the Police, as the Act creates a power to do so, if you believe that someone may be seriously harmed. This would be appropriate in the instance of a suspicion of offences such as murder, rape, kidnapping and causing death by dangerous driving, all of which are arrestable offences.

- **The Crime and Disorder Act (1998)** – Information may be required on an individual if there is a need for strategic cross organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in. A nominated officer deals with such requests.

- **Multi Agency Public Protection (includes the Probation Service)** – The Criminal Justice and Court Services Act 2000, sets the framework for sharing information about potentially dangerous offenders. 'Multi Agency Risk Conferences' may require information about individuals.

  If you are requested to provide information, you should consider gaining consent/informing the individual(s) unless this may cause more harm than good. If the risk presented by an individual(s) clearly cannot be effectively managed without information and gaining consent is inadvisable, then relevant information can be shared as it is in the interest of the public.

  If you suspect a child is being abused, you have a legal power to disclose information to Social Services (under 'vital interest' and 'medical purpose' conditions of the DPA) and/or the Police (under the Police and Criminal Evidence Act). You should consider whether gaining consent or informing the child and parents would be beneficial or detrimental to the situation. If detrimental then disclosure without consent is permitted.

- **Public Health (Control of Diseases) Act 1984** and **Public Health (Infectious Diseases) Regulations 1985** – it is a requirement to disclose information about individuals who have notifiable infectious diseases to various agencies.

- **Births and Deaths Act 1984** – it is a requirement to disclose all births and deaths to local government offices.

Other Acts Preventing Disclosure

1.10 There are also some Acts of Parliament that make it a legal requirement not to disclose information. These Acts are detailed below:

- Human Fertilisation and Embryology Act 2008;

- Venereal Diseases Act 1917 and The NHS (Venereal Diseases) Regulations 1974 and The NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000;

- Abortion Act 1967;

- The Adoption and Children Act 2002.

Appendix E

KEY CONTACT

Job Role	Job Title and Name	Contact Number
Data Security and Protection Team (inc. Freedom of Information) Data Protection Officer	 Paddy Baker	 01305 213567