NHS
Dorset
Clinical Commissioning Group

NHS Dorset Clinical Commissioning Group

CONFIDENTIAL CORPORATE INFORMATION POLICY



Supporting people in Dorset to lead healthier lives

PREFACE

This policy provides staff at all levels with best practice guidance in ensuring that **corporate information** is managed legally and ethically. The purpose of this policy is to ensure that there is a consistent, fair and transparent approach in its application across NHS Dorset Clinical Commissioning Group (CCG). This CCG policy will promote, maintain and strengthen the organisation's strategies and values

This policy **does not** cover the security, use and protection of personal identifiable information as detailed in the Data Protection Act 2018. For the CCG Policy on the use, protection and security of personal identifiable information, please read the Data Security and Protection Policy.

This policy should be read in conjunction with the Data Protection Policy and the Freedom of Information Policy.

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 for NHS Dorset Clinical Commissioning Group to ensure corporate information is managed legally and ethically.	

B	ASSOCIATED DOCUMENTS

- Data Security and Protection Policy
- Data Protection Policy
- Freedom of Information Policy
- IT Security Policy
- Confidentiality: Staff Code of Conduct

C	DOCUMENT DETAILS
Procedural Document Number	19
Author	Paddy Baker
Job Title	Data Protection Officer
Directorate	Finance
Recommending committee or group	Directors
Approving committee or group	Directors
Date of recommendation (version 1)	January 2015
Date of approval (version 1.2)	January 2017
Date of approval (version 1.3)	January 2019
Version	1.3
Sponsor	Chief Finance Officer
Recommendation date	
Approval date	January 2019
Review frequency	Bi-annually
Review date	January 2021

D	CONSULTATION PROCESS		
Version No	**Review Date**	**Author and Job Title**	**Level of Consultation**
1.3	January 2019	Paddy Baker, Data Protection Officer	Directors

E	VERSION CONTROL				
Date of issue	**Version No**	**Date of next review**	**Nature of change**	**Approval date**	**Approval committee/ group**
January 2015	1.1	January 2017	New policy	18 May 2015	Directors
January 2017	1.2	January 2019	Update		Directors
January 2018	1.3	January 2021	Update		Directors

F	SUPPORTING DOCUMENTS/EVIDENCE BASED REFERENCES	
Evidence	**Hyperlink (if available)**	**Date**
NHS Code of Practice: Records Management	www.opsi.gov.uk	2006 updated 2009
BS7799 Industry and adopted NHS IT Security Standards		
Regulations and Investigatory Powers Act	www.opsi.gov.uk	2000
Freedom of Information Act	www.opsi.gov.uk	2000
Crime and Disorder		1998
HSCIC Code of Practice on Confidential Information	www.hscic.gov.uk	2014

G	DISTIBUTION LIST		
Internal CCG Intranet	**CCG Internet Website**	**Communications Bulletin**	**External stakeholders**
√	√	√	Tick as appropriate

CONTENTS		PAGE
1.	Relevant to	**1**
2.	Introduction	**1**
3.	Scope	**1**
4.	Purpose	**2**
5.	Definitions	**2**
6.	Roles and responsibilities	**2**
7.	Security/confidentiality	**3**
8.	Sharing of confidential corporate information	**5**
9.	Privacy impact assessment	**5**
10.	Freedom of Information Act 2000	**5**
11.	Purchase of new equipment, software and systems	**7**
12.	Workforce and organisational development	**7**
13.	Consultation	**7**
14.	Recommendation and approval process	**7**
15.	Communication/dissemination	**7**
16.	Implementation	**7**
17.	Monitoring compliance and effectiveness of the document	**7**
18.	Document review frequency and version control	**7**
APPENDICES		
A	Glossary	**8**

1. RELEVANT TO

1.1 This policy 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, non-executive directors and contracted third parties such as bank, agency, volunteers, locums, student placements, staff on secondment, researchers, visiting professionals and suppliers.

2. INTRODUCTION

2.1 Confidential corporate information belonging to NHS Dorset Clinical Commissioning Group (CCG) is vital to the organisation's success and every employee has a responsibility to use it appropriately, protect its confidentiality and disclose it only if and to the extent authorised to do so.

2.2 Staff within the CCG must also respect the confidentiality of information belonging to others (including providers, stakeholders, suppliers and partners) and not seek, accept or use any confidential corporate information that they know or suspect they are not authorised to have.

2.3 When others provide us with their own confidential corporate information, the CCG must treat it with the same respect that we give our own confidential information and must additionally adhere to any restrictions or conditions upon its use that is required.

2.4 Inappropriate use or disclosure of confidential corporate information can cause serious harm to the CCG and others, damage important relationships, subject employees to disciplinary action and expose employees and the organisation to legal, commercial and reputational harm including damages.

2.5 The CCG has a legal obligation to comply with all appropriate legislation in respect of information handling, information security and confidentiality.

2.6 All staff have a responsibility to familiarise themselves and comply with the conditions described in this policy. Any breaches of this policy will be investigated in line with the CCG disciplinary procedures.

3. SCOPE

3.1 This policy applies to all staff including contracted employees and non-contracted employees such as bank, agency, volunteers, locums, student placements and suppliers.

3.2 This policy covers all aspects of business relating to personal and confidential information within the CCG. Information produced, handled and held by the CCG includes, but is not limited to:

- staff information;
- corporate information;

- service user information.

3.3 This policy covers all methods of holding and transmitting information and in all media, including but not limited to:

- systems purchased, developed and managed by, or on behalf of, the CCG;
- manually stored data in paper format;
- data held in offsite archive storage;
- data held on CDs, memory sticks, laptops, iPads and any other type of mobile media;
- structured and unstructured record systems – paper and electronic;
- transmission of information, including by email, post, fax and telephone.

4. PURPOSE

4.1 The purpose of this policy is to ensure that the CCG will meet its obligations regarding the protection of confidential corporate information.

5. DEFINITIONS

5.1 See Glossary at Appendix A.

6. ROLES AND RESPONSIBILITIES

CCG Governing Body

6.1 The CCG Governing Body supports the legal requirements of the:

- Data Protection Act 2018;
- Freedom of Information Act 2000;
- Regulation and Investigatory Powers Act 2000;
- Investigatory Powers Act 2016;
- Crime and Disorder Act 1998

and endorses this Confidential Corporate Information Policy.

Chief Officer

6.2 The Chief Officer has overall responsibility for the Confidential Corporate Information Policy within the NHS Dorset CCG.

6.3 The Chief Officer will ensure that the CCG has access to specialist advice regarding the requirements of this policy where applicable.

Line Managers

6.4 The day to day responsibility for enforcing this policy is delegated to Line Managers. Managers will ensure that all staff are made aware of the policy.

Director of Engagement and Development

6.5 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 this policy.

Staff

6.6 Staff must keep all corporate CCG documents secure and protect against the unauthorised or inadvertent disclosure of confidential corporate information to other parties. This duty to protect confidential information applies both during and after an individual's employment with the CCG.

6.7 Staff must, prior to disclosing any CCG confidential corporate information to another party, confirm if an agreement is required to protect the information and intellectual property rights of the CCG.

6.8 Staff must keep all confidential corporate information provided to the CCG by other providers/parties protected and secure and only use it within the limits of the authorisation given by the provider/parties.

6.9 When presented with confidential corporate information by anyone other than the owner, staff must confirm that the person providing the information is authorised by the provider/parties to disclose the information.

6.10 Staff must adhere to any relevant laws, regulations or rules applicable in the jurisdictions in which they are operating, including intellectual property laws.

6.11 All CCG employees are responsible for ensuring that all the CCG's corporate/personal data is secured from loss, corruption, damage, disclosure and so on by complying with the law and with this policy and associated policies and procedures.

7. SECURITY/CONFIDENTIALITY

7.1 The CCG must not seek, accept or use any confidential information belonging to another party without authorisation from the provider/parties.

7.2 The CCG must not accept or use any confidential corporate information that the provider/parties have not authorised the CCG to receive, regardless of the form in which such confidential information is communicated (e.g. paper copies, email, oral communication).

7.3 The CCG must not use confidential corporate information other than as authorised by the provider/parties. The CCG will take all reasonable measures to obtain **consent** wherever possible prior to using or sharing information belonging to providers/parties.

7.4 The CCG must not obtain from a third party (e.g. agent, commercial intermediary, adviser, consultant, customer, supplier, joint venture, consortium, partner) any confidential corporate information that the CCG is not authorised to receive.

7.5 The CCG must not seek to obtain confidential corporate information from other providers/parties through illegal, unethical or disreputable means.

7.6 All CCG employees must protect confidential corporate information and must not use or disclose it to any other parties without appropriate authorisation.

7.7 When entrusted with confidential information from other providers/parties, all employees must protect it as they would CCG confidential information and use it only within the limits of the authorisation provided by the owner.

7.8 All staff have a responsibility to ensure that the confidentiality of person identifiable information and confidential corporate information is maintained whilst under their ownership:

- discretion should be used when discussing confidential corporate information in situations where you might be overheard;
- care should be taken to appropriately mark and store documents;
- confidential corporate information must not be stored where it is easily accessible by unauthorised persons;
- communication of confidential corporate information must be by secure means;
- recipients of confidential corporate information must be made aware that it should be treated as such;
- confidential corporate information must only be disclosed to employees and/or third parties when necessary.

7.9 Any possible breaches or risk of breaches identified by staff should be raised with the relevant line manager or relevant director.

7.10 This policy DOES NOT cover the security, use and protection of personal identifiable information as detailed in the Data Protection Act 2018. For the CCG policy on the use, protection and security of person identifiable information, please see the:

- Data Security and Protection Policy;

- Data Protection Policy; and
- IT Security Policy.

8. SHARING OF CONFIDENTIAL CORPORATE INFORMATION

8.1 Where confidential corporate information is to be shared either by the CCG or with the CCG, a confidentiality agreement should be in place wherever possible.

9. DATA PROTECTION IMPACT ASSESSMENT

9.1 In 2008 the Cabinet Secretary commissioned a review of Data Handling Procedures within government in recognition of public interest in the safe handling and sharing of personal data. The report following this review established Privacy Impact Assessments (PIAs) as a requirement for all government departments.

9.2 The introduction of the EU General Data Protection Regulation (GDPR) and the UK Data Protection Bill which became law on 25 May 2018, has made the completion of PIAs, now known as Data Protection Impact Assessments (DPIAs), a mandatory requirement for organisations when carrying out high risk processing.

9.3 The CCG has introduced a DPIA guidance document with screening checklist and DPIA template, based on the documentation issued by the Information Commissioner's Office. A DPIA helps to assess, identify and address any privacy concerns (including corporate privacy concerns) and should be completed at an early stage of a new project/service or when changes are made to existing services.

9.4 The guidance document and template DPIA form is available on the CCG intranet or from the Data Protection team.

10. FREEDOM OF INFORMATION ACT 2000

10.1 The Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations 2004 (EIR) place various requirements on public authorities in relation to information provision and openness. As a public authority, the CCG has obligations under FOIA and EIR.

10.2 FOIA/EIR are part of the Government's commitment to greater openness in the public sector and aims to help transform the culture of the public sector to one of greater openness.

10.3 Whilst the FOIA creates a general right of access to information held, the CCG does not have to comply with information requests where the information requested is exempt under the provisions made in Part II of the FOIA, sections 21-44.

The Public Interest

10.4 The majority of the exemptions set out in the FOIA must only be relied upon if the CCG is satisfied that maintaining the exemption in question outweighs the public interest in disclosure.

10.5 To some, or all of the information requested, the CCG will then have to consider whether it must override the exemption because it is in the public interest to release the information. This public interest test involves considering the circumstances of each particular case and the exemption that covers the information.

Consultation with Third Parties

10.6 The CCG recognises that in some cases the disclosure of information may affect the legal rights of a third party. Unless an exemption applies, the CCG is obliged to disclose that information in response to a request.

10.7 In some cases, disclosure of information cannot be made without the consent of a third party. In this instance the CCG will consult that third party to seek their consent to the disclosure, unless such a consultation is not practicable, for example because the third party cannot be located or because the costs of consulting them would be disproportionate.

10.8 The CCG will consider the requirements of FOIA, the individual circumstances of the request, and decide on the appropriate action. Consultation will be unnecessary where the CCG:

- does not plan to disclose the information requested;
- decides that no exemption applies so the information must be disclosed;
- decides that the third party could not have an effect on the decision to disclose.

10.9 Where the interest of a group of third parties may be affected by disclosure, all reasonable and practical attempts will be made to consult a representative, organisation or individual from these parties, and where one does not exist, to consult a sample representation.

10.10 If the third party does not respond to the consultation, it does not relieve the CCG of its duty to disclose information under the FOIA, or its duty to reply within the time specified.

10.11 In all cases it is for the CCG, not the third party (or representative), to determine whether or not information should be disclosed. A refusal to consent to disclosure by a third party does not mean information should be withheld.

10.12 Any consultation with third parties will take place as soon as is practicable, and the applicant will be informed as soon as possible.

11. PURCHASE OF NEW EQUIPMENT, SOFTWARE AND SYSTEMS

11.1 Managers responsible for CCG projects with a dependency upon IT must complete a project template document (available via the IT Department). This will be used to register the project with the IT Steering Group and to ensure compliance with the legislation. Please refer to the IT Security Policy.

12. WORKFORCE AND ORGANISATIONAL DEVELOPMENT

12.1 All contracts of employment must include a confidentiality clause.

12.2 Students, staff of other agencies, temporary staff and volunteers must sign declarations of confidentiality on commencing employment with the CCG.

12.3 A breach of the requirements of this policy may result in an investigation in line with disciplinary procedures which may lead to a termination of contract and/or legal action.

13. CONSULTATION

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

14. RECOMMENDATION AND APPROVAL PROCESS

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

15. COMMUNICATION/DISSEMINATION

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

16. IMPLEMENTATION

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

17. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE DOCUMENT

17.1 The Data Security and Protection Group takes overall responsibility for ensuring compliance with this policy, reporting to the SIRO and the Caldicott Guardian to ensure Governing Body level assurance.

18. DOCUMENT REVIEW FREQUENCY AND VERSION CONTROL

18.1 This policy will be reviewed bi-annually or earlier if appropriate, to take into account any changes to legislation that may occur.

Appendix A

GLOSSARY

Phrase	Definition
Confidential information	Confidential information is any information that is not in the public domain and is intended to be protected from disclosure. Information may be confidential, irrespective of whether it is specifically labelled 'confidential' or 'proprietary' or otherwise, or whether it is oral, written, drawn or stored electronically. Alternatively, labelling information 'confidential or 'proprietary' or other classification does not automatically make the information confidential information.
Provider/Parties	The provider/parties that own the confidential information and can authorise its disclosure to, and use by another party. The provider/parties are different from just a 'holder' of such information. A holder has been provided with confidential information by the provider/parties but may use it only within the limits of the authorisation given by the provider/parties. Confidential information also includes information obtained from others that the CCG is obligated to keep confidential.