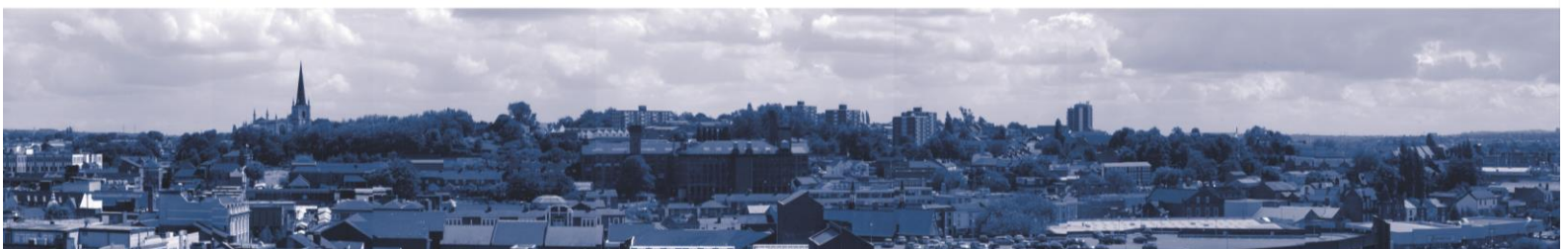
NHS

Walsall Clinical Commissioning Group

Staff Code of Conduct on Confidentiality of Information



Staff Code of Conduct on Confidentiality of Information Walsall Clinical Commissioning Group

The Audit & Governance Committee approved this document on:

Date: 17 September 2018
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	**V5.0**
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer – Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	17 September 2018
Date Policy is Effective From	Date of ratification
Review date:	February 2019
Expiry date:	March 2019
Date of Equality and Diversity Impact Assessment	
Date of Health Inequalities Impact Assessment	
Target audience:	All CCG Staff and persons working on behalf of the CCG
National Documents	Data Protection Act 2018 General Data Protection Regulation Computer Misuse Act 1990 Human Rights Act 1999 The Protection and Use of Patient Information (HSG 96 18) The Caldicott Report 1997 Freedom of Information Act 2000 Common Law Duties of Confidence
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	Date of ratification
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	BCC IG team

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation
Sally Roberts	Director of Governance Quality & Safety
Sara Saville	Head of Corporate Governance

Serena Causer	Corporate Governance Officer

Circulated to the following for consultation

Name/Committee/Group/	Designation
SQP	
IG Functional leads	
SIRO	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments
IG functional lead	Include action for media enquiries Define business information Include details on how to access email policy

Version Control Summary

Significant or Substantive Changes from Previous Version

Version	Date	Comments on Changes	Author
V1.1	Jan 2013	BCC Staff Code of Conduct on Confidentiality was reviewed to reflect WCCG structure and process	Sara Saville Risk and Assurance Manager
V 2.0	Jan 2013	Ratified	Sara Saville
V 3.0	Sept 2015	Ratified	Sara Saville
V4.0	Sept 2017	Ratified	Sara Saville
V4.1	May 2018	Reflect General Data Protection Regulation	Serena Ellis
V4.2	August 2018	Reflect Data Protection Act 2018 and General Data Protection Regulation	Serena Ellis

Contents

1.0 Purpose of Code

1.1 The purpose of this code is to ensure everyone working within Walsall CCG is aware of their responsibilities when using confidential information and maintains the correct relationship with patients, staff and other confidential business of the Organisation, or department.

1.2 For the purpose of this code all data or information that can be related to an identifiable person is considered confidential and must only be used in concurrence with the advice given herein.

1.3 The need to ensure confidentiality of information is and always has been, a major concern of everyone working within the Organisation. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

1.4 The principle behind this code is that no employee shall misuse any information or allow others to do so.

1.5 This code of conduct has been written to meet the following legal requirements and best practice Guidance:

Data Protection Act 2018
General Data Protection Regulation
Computer Misuse Act 1990
Human Rights Act 1999
The Protection and Use of Patient Information (HSG 96 18)
The Caldicott Report 1997
Freedom of Information Act 2000

Common Law Duties of Confidence

2.0 Basic Principle

2.1 Any personal data as defined in Article 4 of the General Data Protection Regulation, given or received in confidence for one purpose may not be used for a different purpose or passed to anyone else without a lawful basis to do so.

2.2 All NHS staff are under a duty of confidence and this has long been established as common law which deals with any unauthorised use or disclosure of confidential information on the basis of actual or implied agreement to keep such information concealed. It is important that patients, public and staff can be assured that information will be handled in the strictest confidence.

2.3 All employees have a contractual obligation to maintain the confidentiality of any information regarding patients and their circumstances that may come into their possession within their job role.

3.0 Information

3.1 In this code, the term “patient information” applies to all personal information about members of the public held by the Organisation. This includes all health records as well as “non health” information.

3.2 In this code, the term “Business information” applies to all commercial information such as details of tenders, prices, contract details and corporate data.

3.3 It is vitally important that patients, staff and the public can be assured that information will be handled in the strictest confidence.

3.4 All employees have a contractual obligation to maintain the confidentiality of any information regarding patients and their circumstances that may come into their possession in the course of their duties.

3.5 Whilst the degree of sensitivity of information will vary, the degree of confidentiality does not. All information about patients must be regarded as confidential. Employees shall not, except as authorised by their line manager or required by their duties under their employment contract, use or divulge to any other employees, firm, or other organisation (whether NHS or not) whatsoever any confidential information about patients which may come to their knowledge during the course of employment or thereafter.

3.6 Staff receiving telephone calls from the public seeking patient or business information should establish whether or not the source is genuine by calling the organisation from where the caller states they are enquiring, or ask that

the request is made in writing. If you are in any doubt regarding requests for patient information please refer to the organisation's Safe Haven Policy.

3.7 Patient Information Systems contain a considerable amount of patient information, which is accessible to staff. Authorised users of the systems can only gain access by password and are:

a) Expected to access the system only to obtain information that they legitimately need to do their job

b) Not authorised to access their own medical records which may be stored on the system; access as a patient but not as member of staff must be applied for through the Data Protection Act 2018 and the General Data Protection Regulation.

c) Required to keep their personal code/password confidential and must not divulge it to anyone. Please refer to the Password Management Policy if there are any queries.

3.8 When any difficulties or doubts do occur in respect of whom disclosures of confidential material ought to be made, staff should be cautious and depending upon the circumstances, seek advice from their manager, the Information Governance Manager Caldicott Guardian or the Data Protection Officer. Staff should not share any information or make comment if they receive enquiries from the press. All enquiries should be immediately directed to the communications department.

4.0 Personal Information/Data on Staff

4.1 Information pertaining to members of staff or anyone working for the Organisation may not be attained by any means which mislead or deceive either current or prospective employees and it should be processed fairly and lawfully. Information on members of staff or anyone working for the Organisation should only be collected for justified reasons and specified purposes. These should normally be communicated in advance, to the employees concerned.

Examples include data which is necessary:

- for compliance with employment law and the administration of an individual's employment contract.
- to establish an employee's training and/or development requirements.
- to assess an employee's qualifications for a particular job or task.
- to gather further evidence where there is a prima facie case for disciplinary action.
- for remuneration policy and payroll administration.
- to establish a contact point in the case of an emergency (next of kin).

4.2 Access to staff records by management should be strictly controlled at all times, on a formal 'need to know' basis.

4.3 Employees have the right (at reasonable intervals) to gain a copy of all personal data about themselves which is held by the Organisation. The request must be clearly stated in writing. An access request should be satisfied within one month from the manager's receipt of details about the personal data being sought.

5.0 Other confidential information

5.1 Staff frequently find that, as part of their job, they have access to confidential reports and information concerning the business of the Organisation. The responsibility to maintain confidentiality applies equally to business information as it does to patient and staff information.

5.2 If a member of the public would like access to any business/corporate information they should apply in writing, which will be processed in line with their rights under the Freedom of Information Act 2000.

6.0 Email Policy and Code of Conduct

6.1 All Organisation employees who use computers to carry out their duties should ensure that they have read the Email Policy and Code of Conduct and comply with any applicable procedures. If an employee has not been given a copy they should obtain a copy of this policy from their Manager. The email policy is section 6.16 of the IMT policy which can be sourced from reception or the Corporate Governance Officer 01922 618318.

7.0 Failure to maintain confidentiality

7.1 The obligation to maintain confidentiality is both an expressed and implied condition of service for all staff.

7.2 The Organisation takes its responsibilities extremely seriously in respect of monitoring confidentiality. Any employee found to be breaking the rules for accessing computerised information, or in passing on any information to persons not having the right to it, will be deemed to have breached their contract. Alleged breaches of the Code of Conduct will be promptly considered and justly investigated. If the accountable officer or senior managers are to be investigated the Organisation should use individuals who are employed elsewhere to conduct the investigation. Contravention will result in disciplinary action being taken under the procedure for dealing with major offences and could result in dismissal.

8.0 Disposal of Confidential Paper Records and Electronic Records

8.1 Staff must ensure that when disposing of confidential paper records, such material is either shredded, placed in confidentiality bags or the confidentiality bins provided as appropriate to observe the regulations laid down by the Data Protection Act 2018 and the General Data Protection Regulation.

9.0 Disposal of Hard Drives

9.1 Staff must ensure that confidential information that is stored upon hard drives is disposed of via the IT department.

10.0 Responsibility for Passing on Information

10.1 staff are individually responsible for deciding to pass on information. If staff are unsure whether to pass on information the manager or Information Governance Manager should be consulted.

10.2 The unauthorised disclosure of patient, staff or any other Organisational business information by any member of staff is a serious matter and may result in disciplinary action and possible legal action.

11.0 Non-identifiable Information (Anonymised)

11.1 Where anonymised information would be sufficient, identifiable information should be omitted where possible. Do not use patient identifiable information unless it is essential for the purpose.

12.0 Monitoring Compliance

12.1 Staff are expected to comply with the requirements set out within the Freedom of Information Policy and related Policies. Compliance will be monitored via Manager and Information Governance reports, spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of Data Security and Protection Toolkit.

12.2 Non adherence to the Freedom of Information Policy and related Policies will result in local Disciplinary Policies being implemented.