Information Governance Policy

Queen Camel Medical Centre

January 2020

Reviewed January 2022

Contents

1. Introduction and Purpose

The role of the Queen Camel Medical Centre (the Practice) is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the Practice will uphold the NHS Constitution. This policy is important because it will help the people who work for the Practice to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection Legislation assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

The aims of this document are to maximise the value of practical assets by ensuring that information is:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

To protect the practice's information assets from all threats, whether internal or external, deliberate or accidental, the Practice will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met

- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff

2. Scope and Definitions

Scope

The scope of this document covers:

- All permanent employees of the Practice and;
- Staff working on behalf of the Practice (this includes contractors, temporary staff, and secondees).

The Practice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Practice fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The Practice also recognises the need to share information in a controlled manner. The Practice believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

Definitions

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents.

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural 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 Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition

	(h) Their sexual life
Personal Confidential Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to the Practice or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

3. Legal Compliance

The Practice regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The Practice will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulation (GDPR), the Data Protection Act (DPA) 2018, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time.

In addition, consideration will also be given to all applicable Law concerning privacy, confidentiality, the processing and sharing of personal data including the Human Rights Act 1998, the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations.

The Practice when acting as a Controller, will identify and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ' 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 Queen Camel Medical Centre will identify the official authority (legal basis) and record this on relevant records of processing.

The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic.

Queen Camel Medical Centre will help the people who use our services to understand that they can opt out of their data being used for other purposes. Our policies, procedures, and privacy notice cover the opt out.

All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 31 March 2022.

4. Roles and Responsibilities

The Practice has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements. The Practice is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Practice Management

It is the role of the Practice Manager to define the Practice policy in respect of Information Governance, taking into account legislative and NHS requirements. The Practice Manager is also responsible for;

- ensuring that sufficient resources are provided to support the requirements of the policy
- appropriate mechanisms are in place to support service delivery and continuity

The Practice Manager is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Information Governance in the Practice and raising awareness of Information Governance.

All staff have responsibility for complying with this policy and with Data Protection Legislation, the following roles have specific responsibilities:

The management of information risk and information governance practice is now required within the Statement of Internal Control which the Accountable Officer is required to sign annually.

Caldicott Guardian

The Caldicott Guardian is the person within the Practice with overall responsibility for protecting the confidentiality of personal data and special categories of personal data (described as Personal Confidential Data (PCD)) in the Caldicott 2 report, and for ensuring it is shared appropriately and in a secure manner. This role has the responsibility to advise the Practice on confidentiality issues.

Data Protection Officer

The Data Protection Officer (DPO) is the person that has been identified that has the responsibilities as set out in the GDPR guidance, such as monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the practice and acting as the contact point with the and ICO.

5. Processes/Requirements

The Practice will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about the Practice and its services will be available to the public through a variety of media.

The Practice will maintain policies to ensure compliance with the Freedom of Information Act.

The Practice will have clear procedures and arrangements for liaison with the press and broadcasting media. All media enquiries should be made to the Practice Manager.

The Practice will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to the Practice's Individual Rights Policy in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018.

The Practice will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016). Please refer to The Practice Records Management Policy.

6. Information Security

The Practice will maintain policies for the effective and secure management of its information assets and resources.

The Practice will promote effective confidentiality and security practice to its staff through policies, procedures and training. Please refer to the Practice Information Security, Remote Working and Portable Devices and Network Security policies.

The Practice will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the practice becomes aware of the incident. Please refer to The Practice Incident Reporting Policy.

7. Information Quality Assurance

The Practice will maintain policies and procedures for information quality assurance and the effective management of records.

The Practice will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Staff are expected to take ownership of, and seek to improve, the quality of information within the Practice.

Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

8. Commissioning of New Services

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the Practice Management Team.

All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA.

The Practice will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

9. Training

All new starters to the Practice inclusive of temporary, bank staff and contractors must undertake Information Governance induction training via the eLfH website to evidence compliance with the Data Protection Legislation and the DSP Toolkit assertions as part of the induction process. Extra training will be given to those dealing with requests for information. A register will be maintained of all staff who have completed the online training and those who have attended face to face training sessions where these are offered.

Annual IG training should be undertaken by all staff.

10. Monitoring and Review

This policy will be monitored by the Practice Manager to ensure any legislative changes that occur before the review date are incorporated.

Compliance with Practice policies is stipulated in staff contracts of employment. If staff members are unable to follow Practice policies or the policy requirements cannot be applied in a specific set of circumstances, this much be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with Practice policies or failure to report non-compliance may be treated as a disciplinary offence.

This policy will be reviewed annually by the Practice Manager, or if required by law.

11. References and Associated Codes of Practice

- NHS Digital Codes of Practice
- Department of Health Code of Practice
- CQC Code of Practice
- Health and Social Care (Safety and Quality) Act 2015
- NHS England Policy
- All Practice policies, procedures and guidance relating to the management and processing of information within the organization
- National data opt-out operational policy guidance document - NHS Digital

12. Public Sector Equality Duty – Equality Impact Assessment

An Equality Impact Assessment has not been completed.

Appendix A: Staff Guidance on Identifying and Reporting an Information Incident

This guidance applies to all staff including permanent, temporary and contract staff.

All incidents must be reported to your line manager immediately once you become aware of the incident. The Data Protection Officer should as a minimum be informed within 24 hours or 1 working day of you becoming aware of the incident.

Where an incident occurs out of business hours, the designated on-call officer will ensure that action is taken to inform the appropriate contacts within 24 hours of becoming aware of the incident.

The Incident reporting form at Appendix B must be completed and forwarded to the Practice Data Protection Officer.

What should you report?
There are three types of breaches defined under the Article 29 Working Party which informed the drafting of the General Data Protection Regulation (GDPR):

- Confidentiality breach- unauthorised or accidental disclosure of, or access to personal data

  Example - Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals. If the attacker has not accessed personal data the breach would still represent an availability breach and require notification if the potential for a serious impact on the rights and freedoms of the individual.

- Availability breach- unauthorised or accidental loss of access to, or destruction of, personal data

  Example - In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled. This is to be classified as an availability breach.

- Integrity breach - unauthorised or accidental alteration of personal data

  Example - Where a health or social care record has an entry in the wrong record (misfiling) and has the potential of significant consequences it will be considered an integrity breach. For example, a 'do not resuscitate' notice on the wrong patient record may have the significant consequence of death whilst an entry recording the patient blood pressure may not have the same significant result.

Here are some more examples of information incidents that should be reported:

- You find a computer printout containing Confidential Data laying around;
- You Identify or are informed that a fax that was thought to have been sent to an intended recipient had been received by an unknown recipient or organisation;

- You find confidential waste in a 'normal' waste bin;
- You lose or temporarily misplace a mobile computing device or mobile phone that may have personal information on it;
- Information has been given to someone who should not have access to it – verbally, in writing or electronically;
- A computer database has been accessed using someone else's authorisation e.g. someone else's user id and password;
- A secure area has been accessed using someone else's swipe card or pin number when not authorised to access that area;
- A PC and/or programmes aren't working correctly – potentially because the device may have a virus;
- A confidential or sensitive e-mail has been sent to an unintended recipient or 'all staff' by mistake;
- A colleague's password has been written down on a 'post-it' note and found by someone else;
- A physical security breach ('break in') to the organisation is discovered;
- A phishing email has been received
- A Website has suffered from defacement

What happens next?

The incident will be investigated by the Controller but can be supported to do this by other organisations. The Controller retains the legal obligation to report and investigate incidents.

Where an incident involves data or information that is processed by an organisation on behalf of the Controller, the DPO for the Controller should be informed by the Processor of the potential breach and in addition to providing support for any necessary notification to third parties, agree an appropriate investigation plan. The same must apply where Data Sharing Agreements are in place and notification of potential breaches to agreement partners forms part of each organisation's obligations under that agreement.

The purpose of an incident investigation is to:

- Carry out a root cause analysis in order to establish what actually happened and what actions and recommendations are needed to be taken to prevent reoccurrence;
- To identify whether any deficiencies in the application of Practice policies or procedures and/or Practice arrangements for confidentiality and data protection contributed to the incident;
- Determine whether a human error has occurred, but not to allocate blame;
- Decide whether to notify the data subject. This decision will be made by the Caldicott Guardian on the recommendation of the Data Protection Officer;
- In some cases the investigation may identify whether any disciplinary processes may need to be invoked.

Assessing the severity of an incident
An initial assessment of the incident will be made using the NHS Digital Data Security and Protection Incident Reporting tool.

Notifiable breaches are those that are likely to result in a high risk to the rights of freedoms of the individual (data subject). The scoring matrix used in the reporting tool has been designed to identify those breaches that meet the threshold for notification.

The factors for assessing the severity level of incidents are determined by:

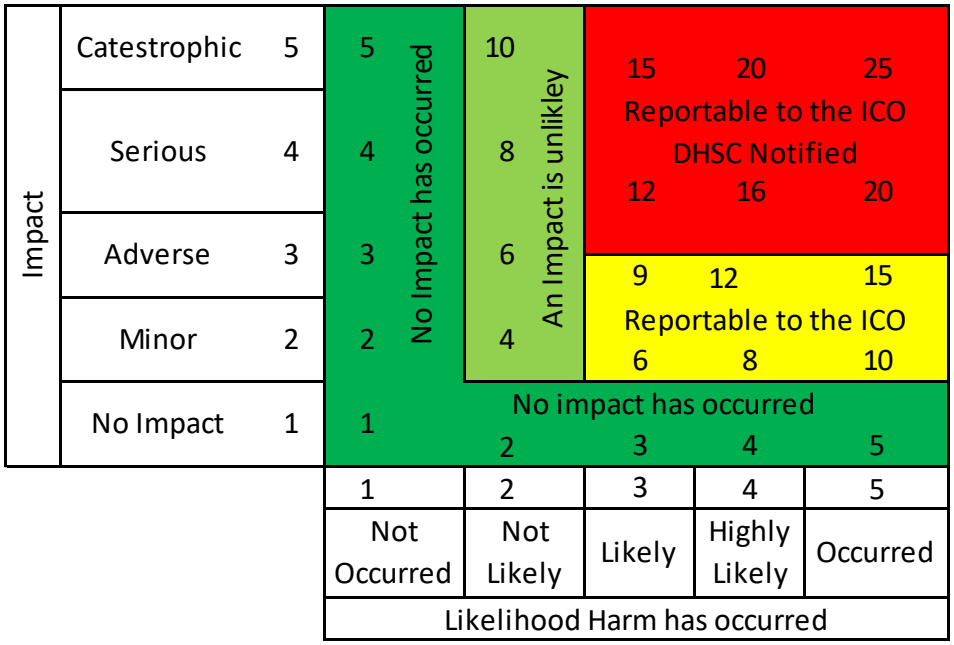
- the potential significance of the adverse **effect** on individuals graded from 1 (lowest) to 5 (highest);

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially Some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

- the **likelihood** that adverse effect has occurred graded from 1 (non-occurrence) to 5 (occurred);

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.

	even if no adverse effect occurred	
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.



Sensitivity factors have been incorporated into the grading scores and where a non ICO notifiable personal data breach involves one of the following categories of data, the breach assessment must start at 'minor impact' and 'harm not likely' scoring it at 2 x 2 = 4. It will only be reportable to the ICO where further assessment increases along the likelihood of harm axis i.e. scores of 6 and above:

- Vulnerable children
- Vulnerable adults
- Criminal convictions/prisoner information including the alleged commission of offences by the data subject or proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing
- Special characteristics listed in the Equality Act 2010 where not explicitly listed in this guidance and it could potentially cause discrimination against such a group or individual
- Communicable diseases as defined by public health legislation
- Sexual health
- Mental health
- Special Categories of personal data

Under the following circumstances notification may not be necessary;

- Encryption – Where the personal data is protected by means of encryption.
- 'Trusted' partner - where the personal data is recovered from a trusted partner organisation. The controller may have a level of assurance already in place with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches.
- Cancel the effect of a breach - where the controller is able to null the effect of any personal data breach.

Assessing the risk to the rights and freedoms of a data subject

The GDPR gives interpretation as to what might constitute a high risk to the rights and freedoms of an individual. This may be any breach which has the potential to cause one or more of the following;

- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft
- Fraud
- Financial loss
- Unauthorised reversal of pseudonymisation
- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other significant economic or social disadvantage to individuals

Internal Reporting

Any information incident that takes place that is not reportable will still be included in reports circulated to the practice team. These are primarily for staff awareness and to identify trends in minor incidents.

IG incident reports will also be presented to the relevant committees in order to provide assurance that appropriate controls are in place and that IG risks are managed effectively.

Appendix B: Information Governance Incident Reporting Form

Information Governance Incident Reporting Form

Please complete and submit this form to the Practice Manager

Name:-	Date :-

For Internal IG incidents	**For External IG Incidents**	**Details**
	Type of Organisation *(NHS Provider, Contractor etc.)*	
Team *(Governance, PMO etc.)*	Sender *(Organisation name)*	
Location *(where did the incident happen)*	Location *(where did the incident happen)*	
Category *(Post, Memory stick, email etc.)*	Category *(Post, Memory stick, email etc.)*	
Description *(What happened, type of information, no. of recipients, no. of patients etc.)*	Description *(What happened, type of information, no. of recipients, no. of patients etc.)*	
Actions Taken	Actions Taken	

Please ensure all information pertaining to the incident is securely stored until advised by the assigned investigator.

Investigator	
Incident Number	
5x5 matrix score	

Section 2 – Incident Grading *to be completed by the Practice Manager*

Incident Number		Date Received and logged	
Date reported to the Data Protection Officer			
Date reported on the DSP toolkit			
Detail any other stakeholders (Controllers/Processors) and when they have been notified *add extra lines if necessary	**Controller**		**Date notified**
Initial Incident grading and reasoning			
What further information has been gathered since notification and when?			
Final Incident grading and reasoning			

Section 3 – Investigation Details *to be completed by investigating manager*	
Causes and contributory Factors	
Process issues raised	
Lessons learnt & recommendations	

Section 4 – Actions/Learning *to be completed by investigating manager*			
Action	**Responsible**	**Date for completion**	**Completed date**
1.			
2.			
3.			
Date Investigation Report Completed			
Date incident closed			