Data Protection Policy

Version Control

Date	Version Number	Stage	Author
16th September 2014	1.0	Creation	Tim Crowson
30th October 2014	1.1	Review before presentation to Clinical Governance Group	Paul Haycox
5th November 2014	2.0	Inclusion of comments from Sharon Leach	Paul Haycox
29th March 2016	2.1	Change of IT manager	Paul Haycox and Jamie Darlington
26th August 2016	2.2	Minor changes and added reference to EU GDPR	Paul Haycox
19th January 2018	2.3	Reviewed in readiness for GDPR, but requires review in April 2018 when Information Alliance Guidance on GDPR and Data Protection Act 2018 is made available	Paul Haycox
4th May 2018	3.0	Amended Data Protection Principles in line with GDPR; amended the Roles and Responsibilities in line with the GDPR; inserted section on GDPR; amended employee responsibilities and monitoring section.	Paul Haycox
23rd May 2018	3.1	Name change. Addition regarding Privacy Notices	Paul Haycox
12th December 2019	4.0	Added detail regarding legal right for data processing, and roles and responsibilities	Paul Haycox
4th June 2021	4.1	Added national data opt out paragraph GDPR rights	Paul Haycox
10th May 2023	4.2	Old monitoring dates removed DPIA templates added	

Contents

1. Background
2. Data Protection Principles
3. Underpinning Policies and Procedures
4. The General Data Protection Regulation 2018 and Data Protection Act 2018
5. Scope
6. Roles and Responsibilities
7. Employee Responsibilities
8. National Data Opt-out
9. Distribution and Implementation
10. Monitoring

Appendix 1 – DPIA Templates

1. Background

St Michael's Clinic needs to collect personal information about people with whom it deals to carry out its business and provide its services.

Such people include patients, employees (present, past and prospective), suppliers and other business contacts.

The information includes personal data and at times special categories of information. We may occasionally be required to collect and use certain types of such information to comply with the requirements of the law.

No matter how it is collected, recorded and used (e.g. on a computer or on paper) the clinic will seek to make it transparent to individuals

- what is held,
- how it is used,
- who else has access

- the individuals rights
- the legal basis for processing and
- to keep the data as securely as possible

and ensure compliance with the General Data Regulation and Data Protection Act 2018 (the Act).

The lawful and proper treatment of personal information by St Michael's Clinic is extremely important to the success of our business and to maintain the confidence of our service users and employees. We ensure that the St Michael's Clinic treats personal information lawfully and correctly.

2. Data Protection Principles

St Michael's Clinic fully supports and complies with the principles of the GDPR and 2018 Act which are summarised below:

Personal data shall be processed fairly and lawfully and in a transparent manner in relation to the data subject.

Personal data shall be collected for specific, explicit and legitimate purposes.

Personal data held must be adequate, relevant and limited to what is necessary.

Personal data must be accurate and kept up to date. Every reasonable strep will be taken to ensure that personal data that is inaccurate is rectified. Request for personal data to be erased will be considered in line with the reason for which that data is held.

Personal data shall not be kept in a form which permits identification of data subjects for longer than necessary and in accordance with national retention schedule guidance.

Personal data must be kept secure and will be protected with appropriate technical and/or organisational measures.

Personal data shall not be transferred outside the European Economic Area (EEA) unless there is adequate protection.

We uphold the personal data rights outlined in the GDPR;

The right to be informed

The right of access

The right to rectification

The right to erasure

The right to restrict processing

The right to data portability

The right to object

Rights in relation to automated decision making and profiling.

We acknowledge our accountability in ensuring that personal data shall be:

Processed lawfully, fairly and in a transparent manner;

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

Accurate and kept up to date;

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation');

Processed in a manner that ensures appropriate security of the personal data.

3. Underpinning Policies and Procedures

This policy is underpinned by the following:

Data Quality Policy – outlines procedures to ensure the accuracy of records and correction of errors.

Confidentiality Policy – details transparent procedures, the management of records from creation to disposal, information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.

Information Systems Security Policy – outlines procedures for ensuring the security of data and staff responsibilities.

Business Continuity Plan – outline the procedures in the event of a security failure of disaster affecting digital systems or mass loss of information necessary to the day to day running of our organisation.

Staff Data Security Code of Conduct – provides staff with clear guidance on the disclosure of personal information.

4. The General Data Protection Regulation 2018 and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 makes it incumbent on the Data Controller to be able demonstrate compliance with them.

The clinic will evidence compliance with the data protection principles in section 2 through the use of policies, procedures, assessments and plans. These will be held in the Data Protection and Security Toolkit (DSPT), which is updated annually. The

responsibility for updating the DSPT will fall to the Data Controller, IT Manager and Business Manager.

The clinic processes special category data, particularly data relating to health. Data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Health data can therefore include a wide range of personal data, for example:

- any information on injury, disease, disability or disease risk, including medical history, medical opinions, diagnosis and clinical treatment;
- medical examination data, test results, data from medical devices, or data from fitness trackers;
- information collected from the individual when they register for health services or access treatment;
- appointment details, reminders and invoices which tell you something about the health of the individual. These fall under 'the provision of health care services' but must reveal something about a person's health status. For example, a GP or hospital appointment in isolation will not tell you anything about a person's health as it may be a check-up or screening appointment. However, you could reasonably infer health data from an individual's list of appointments at an osteopath clinic or from an invoice for a series of physiotherapy sessions; and
- a number, symbol or other identifier assigned to an individual to uniquely identify them for health purposes (e.g. an NHS number, or Community Health Index (CHI) number in Scotland), if combined with information revealing something about the state of their health.

The clinic processes data under the GDPR Article 9 (2) (h) condition of health and social care

"processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

and the Data Protection Act Schedule 1, condition 2

"the provision of healthcare"

Article 9(3) of the GDPR contains the additional safeguard that you can only rely on this condition if the personal data is being processed by (or under the responsibility of) a professional who is subject to an obligation of professional secrecy. Section 11 of the DPA 2018 makes it clear that in the UK this includes:

(a) a health professional or a social work professional;

Where a health professional includes in its definition doctors and nurses

The clinic has issued a Privacy Notice for both patients and staff members, which outlines the legal basis for processing the data, access to personal data, the individuals rights and contact details for the Data Protection Officer (dpo@stmichaelssclinic.co.uk)

The clinic will continue to assess any guidance and clarification of the law in 2019/20. Any significant guidance will be implemented, and processes, policies, procedures and reporting refined in line with the developing understanding and interpretation of the GDPR and Data Protection Act 2018.

5. Scope

All St Michael's Clinic staff are within the scope of this document, including contractors, temporary staff, secondees and all permanent employees.

6. Roles and Responsibilities

St Michael's Clinic will: -

Ensure that there is always one person with overall responsibility for data protection and appoint a Data Controller. Currently this is Dr Stephen Murdoch. He has overall accountability for establishing and maintaining a safe and effective data management system that adheres to all statutory and regulatory guidelines.

Ensure all types of data held by the clinic is understood and logged.

Ensure all data flows are mapped.

Ensure all data is processed lawfully, with a lawful basis of processing documented and communicated.

Have methods by which the rights of individuals in relation to data held by the clinic are informed to them. This will be through a clearly worded Privacy Notices. Privacy Notices will be referenced in all clinic letters for new appointments; will be displayed in the clinics reception area; be available on the clinics internet site and through paper copies held at the clinic. Employees will be notified of the relevant notice and it will be displayed in staff areas and available on the company's intranet.

Have a process for ensuring data subjects can access their data within the time frames required. This will include the ability to log and report on the numbers of requests. No barriers will be placed on people requesting data, other than ensuring that they are the relevant person who has a right to that data.

Have a process for ensuring the data held is up to date and accurate. Any inaccuracies brought to the attention of the clinic by data subjects are reviewed, rectified and/or erased (subject to the outcome of the review and the reason the data is held).

Have a process for restricting processing of data - at the request of an individual and subject to a review and the reason the data is held

Have a process for ceasing the processing of data - at the request of an individual and subject to a review and the reason the data is held

Appoints a Data Protection Officer to support the monitoring of compliance of the GDPR

Provide training for all staff members who handle personal information

Provide clear lines of report and supervision for compliance with data protection

Carry out regular checks to monitor current systems and to assess new processing of personal data.

To ensure a Data Protection Impact Assessment is undertaken for any significant new projects which will impact of Data Protection

To hold an Information Risk log

To ensure policies are in place that relate to the security of data held and transferred. This will include formal contractual arrangements with data processors.

To ensure data breaches are reported within the required timescales.

In line with legislation we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

7. Employee Responsibilities

All employees will, through appropriate training and responsible management:

Processed lawfully, fairly and in a transparent manner;

Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

Accurate and kept up to date;

Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);

Processed in a manner that ensures appropriate security of the personal data.

Observe all forms of guidance, codes of practice and procedures about the collection and use of personal information.

Understand fully the purposes for which the St Michael's Clinic uses personal information.

Collect and process appropriate information, and only in accordance with the purposes for which it is to be used by the St Michael's Clinic to meet its service needs or legal requirements.

Ensure the information is correctly input into the St Michael's Clinic systems.

Ensure the information is destroyed (in accordance with the provisions of the Act) when it is no longer required.

On receipt of a request from an individual for information held about them by or on behalf of immediately notify the Data Protection Officer, Mr Paul Haycox.

Not send any personal information outside of the United Kingdom without the authority of the Caldicott Guardian.

Understand that breaches of this Policy may result in disciplinary action, including dismissal.

8. National Data opt-out

Under the national data opt-out everyone who uses publicly-funded health and/or care services can stop health and care organisations from sharing their "confidential patient information" with other organisations if it is not about managing or delivering their own care. For example, if this information is used for research or planning purposes.

St Michael's Clinic have no uses or disclosures which need to have national data opt-outs applied. However future uses or disclosures will be checked against the national data opt-out operational policy guidance. If it is deemed that the national opt out technical solution is required St Michael's will be ready to implement the NHS Digital MESH mail system using the appropriate spreadsheets.

This does not affect how we share information with other organisations to manage someone's care and it won't apply if we have explicit consent to share information or if the information is appropriately anonymised.

9. Distribution and Implementation

This document will be made available to all Staff via the St Michael's Clinic intranet site.

A global notice will be sent to all Staff notifying them of the release of this document.

The document will be emphasised in any training.

10. Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Senior Clinicians and Managers meeting.

The Business Manager is responsible for the monitoring, revision and updating of this document on a 3 yearly basis or sooner if the need arises.

Appendix 1

St Michaels Clinic

Data Protection Impact Assessment Procedure

Version Control

Date	Version	Stage	Author
28th February 2019	1.1	Creation	Paul Haycox
18th March 2019	2.0	Ratified by CGM	Clinical Governance Group
March 2021	2.1	Amended in relation to DPA/GDPR and ICO guidance	Paul Haycox
May 23	2.1	No Change	Paul Haycox

Contents

1. Introduction 3
2. Purpose 3
3. Scope 4
4. Key Roles and Responsibilities 4
5. Process 5
    5.1 Full scale Data Protection Impact Assessment 5
6. Monitoring and Review 6
7. Training 6
8. Distribution and Implementation 6
9. Associated Legislation and Documents 6
10. References 7
11. DPIA screening checklist 8
    DPIA process checklist 9
    Have we written a good DPIA? 10

1. Introduction

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

A Data Protection Impact Assessment (DPIA) should be carried out whenever there is a change that is likely to involve a new use; or significantly change the way in which personal data is handled, and there is likely to result in a high risk to individuals - for example a redesign of an existing process or service, or a new process or information asset is being introduced.

This document is a practical tool to help identify and address the data protection and privacy concerns at the design and development stage of a project or significant change - building data protection compliance in from the outset. It sets out St Michaels Clinic procedure for conducting a DPIA through a project lifecycle to ensure that, where necessary, personal and sensitive information requirements are complied with and risks are identified and mitigated

2. Purpose

A DPIA must be completed before the clinic begins any type of processing that is "likely to result in a high risk". This means that although the actual level of risk is not fully assessed, the clinic needs to screen for factors that point to the potential for a widespread or serious impact on individuals.

In particular, the UK GDPR says you must do a DPIA if you plan to:

- use systematic and extensive profiling with significant effects;
- process special category or criminal offence data on a large scale; or
- systematically monitor publicly accessible places on a large scale.

When considering if processing is likely to result in high risk, you should consider the relevant European guidelines. These define nine criteria of processing operations likely to result in high risk. While the guidelines suggest that, in most cases, any processing operation involving two or more of these criteria requires a DPIA, you may consider in your case that just meeting one criterion could require a DPIA.

The ICO also requires a DPIA if you plan to:

- use innovative technology (in combination with any of the criteria from the European guidelines);
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data (in combination with any of the criteria from the European guidelines);
- process genetic data (in combination with any of the criteria from the European guidelines);
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice ('invisible processing') (in combination with any of the criteria from the European guidelines);

- track individuals' location or behaviour (in combination with any of the criteria from the European guidelines);
- profile children or target marketing or online services at them; or
- process data that might endanger the individual's physical health or safety in the event of a security breach.

This template is based on the Information Commissioners Office guidance on implementation and use of DPIAs and has been adapted for use within the clinic.

Under the General Data Protection Regulation (GDPR) this is an express legal requirement.

This document is a statement of the approach and intentions for St Michaels Clinic to fulfil its statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives.

3. Scope

This document applies to all staff, whether permanent, temporary or contracted. They are responsible for ensuring that they are aware of all relevant requirements and that they comply with them on a day to day basis.

Furthermore, the principles of this document apply to all third parties and others authorised to undertake work on behalf of St Michaels Clinic.

This document covers all aspects of information, in both paper and electronic format.

4. Key Roles and Responsibilities

Role	Responsibility
Seniors meeting	The seniors meeting have ultimate accountability for actions and inactions in relation to this document
Senior Information Risk Officer	St Michaels Clinic SIRO is responsible for having overall accountability for Information Governance; this includes the Data Protection and Confidentiality function. The role includes briefings and providing assurance that the IG approach is effective in terms of resource, commitment and execution. The SIRO for St Michaels Clinic is the Business Manager.
Caldicott Guardian	The Caldicott Guardian has responsibility for ensuring that there are adequate standards for protecting patient information and that all data transfers are undertaken in accordance with Safe Haven guidelines and the Caldicott principles. The Caldicott Guardian for St Michaels Clinic is Mark Norfolk.
Data Protection Officer	The DPO has responsibility for Data Protection compliance and is Amanda Copeland
IT Manager	The IT Manager has day to day responsibility for implementing and monitoring procedures to ensure compliance with relevant information legislation The IT Manager is responsible for overseeing completed data protection impact assessments and advising on identified risks and mitigations
Senior nurses and doctors	Senior nurses and doctors are responsible for ensuring that staff who report to them have suitable access to this document and it's supporting policies and procedures and that they are implemented in their area of authority.
All staff	Have a responsibility to: • Be aware of the Information Governance requirements • Support St Michaels Clinic to achieve Toolkit Compliance • Complete annual IG training • Report information Incidents appropriately

5. Process

Any systems which do not identify individuals in any way do not require a DPIA to be performed. However, it is important to understand that what may appear to be "anonymised" data, could in fact be identifiable when used with other information, so anonymised data should be considered very carefully before any decision is made that it will not identify individuals. Any person who is responsible for introducing a new or revised service or changes to a new system, process or information asset is the Information Asset Owner (IAO) and is responsible for ensuring the completion of a DPIA if the criteria in section 2 is met.

5.1 Full scale Data Protection Impact Assessment

In most small-scale projects, the DPIA may identify one or more IG risks and the lead manager will be advised on the actions necessary to mitigate or eliminate those risks.

Where the DPIA discovers complex or several IG risks, an action plan should be developed on how the risks will be mitigated and a report should be produced. The final report should cover (where applicable):

- A description of the proposal including the data flow process
- The case justifying the need to process an individual's personal
- An analysis of the data protection issues arising from the project
- Details of the parties involved
- Details of the issues and concerns raised
- Discussions of any alternatives considered to meet those concerns and the rationale for the decisions made
- An analysis of the public interest of the scheme
- Compliance with the data protection principles
- Where the proposal involves the transfer and storage of personal data the PIA should include details of any security measures that will be put into place to ensure the data is protected and kept secure.

The organisations Caldicott Guardian and/or Senior Information Risk Owner (SIRO) should be included at an early stage to ensure adequate consultation of the DPIA.

6. Monitoring and Review

Performance against key performance indicators will be reviewed on an annual basis through the DPS Toolkit submission and used to inform the development of future documents.

Unless there is major legislation or policy, this document will be reviewed every two years.

7. Training

Appropriate Data Security and Protection training will be provided to all staff annually.

8. Distribution and Implementation

All policy and procedural documents in respect of Information Governance will be made available via the St Michaels Clinic staff intranet.

Staff will be made aware of procedural updates as they occur via notification on the St Michaels Clinic staff intranet.

9. Associated Legislation

The following references and areas of legislation should be adhered to.

- Confidentiality NHS Code of Practice
- Data Protection Act 1998
- Caldicott Guardian principles
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Health Records 1990
- Records Management NHS Code of Practice
- UK General Data Protection Regulation (UKGDPR)

10. References

Information Commissioner's Office PIA Code of Practice
https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf

The DSPT Toolkit
Data Security and Protection Toolkit - NHS Digital

Data Protection Act 1998
http://www.legislation.gov.uk/ukpga/1998/29/contents

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/contents

Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation
https://www.dsptoolkit.nhs.uk/Help/Attachment/148

The NHS Constitution for England
NHS Constitution for England - GOV.UK (www.gov.uk)

NHS Code of Confidentiality
Confidentiality: NHS Code of Practice - GOV.UK (www.gov.uk)

NHS Keeping patient records safe and secure
https://www.nhs.uk/nhsengland/thenhs/records/healthrecords/documents/patientguidancebooklet.pdf

NHS Information Risk Management
https://digital.nhs.uk/about-nhs-digital/our-organisation/our-organisation-structure/assurance-and-risk-management

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/publications/the-information-governance-review OK

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/contents OK

11. DPIA screening checklist

DPIA Awareness

☐ We provide training so that our staff understand the need to consider a DPIA at the early stages of any plan involving personal data.

☐ Our existing policies, processes and procedures include references to DPIA requirements.

☐ We understand the types of processing that require a DPIA and use the screening checklist to identify the need for a DPIA, where necessary.

☐ We have created and documented a DPIA process.

☐ We provide training for relevant staff on how to carry out a DPIA.

DPIA Screening

☐ We consider carrying out a DPIA in any major project involving the use of personal data.

☐ We consider whether to do a DPIA if we plan to carry out any other:

- ☐ evaluation or scoring;
- ☐ automated decision-making with significant effects;
- ☐ systematic monitoring;
- ☐ processing of sensitive data or data of a highly personal nature;
- ☐ processing on a large scale;
- ☐ processing of data concerning vulnerable data subjects;
- ☐ innovative technological or organisational solutions;
- ☐ processing that involves preventing data subjects from exercising a right or using a service or contract.

☐ We always carry out a DPIA if we plan to:

- ☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;
- ☐ process special-category data or criminal-offence data on a large scale;
- ☐ systematically monitor a publicly accessible place on a large scale;
- ☐ use innovative technology in combination with any of the criteria in the European guidelines;
- ☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- ☐ carry out profiling on a large scale;

☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;

☐ combine, compare or match data from multiple sources;

☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;

☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;

☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;

☐ process personal data that could result in a risk of physical harm in the event of a security breach.

☐ We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

☐ If we decide not to carry out a DPIA, we document our reasons.

DPIA Progress Checklist

☐ We describe the nature, scope, context and purposes of the processing.

☐ We ask our data processors to help us understand and document their processing activities and identify any associated risks.

☐ We consider how best to consult individuals (or their representatives) and other relevant stakeholders.

☐ We ask for the advice of our data protection officer.

☐ We check that the processing is necessary for and proportionate to our purposes and describe how we will ensure compliance with data protection principles.

☐ We do an objective assessment of the likelihood and severity of any risks to individuals' rights and interests.

☐ We identify measures we can put in place to eliminate or reduce high risks.

☐ We record our decision-making in the outcome of the DPIA, including any difference of opinion with our DPO or individuals consulted.

☐ We implement the measures we identified and integrate them into our project plan.

☐ We consult the ICO before processing, if we cannot mitigate high risks.

☐ We keep our DPIAs under review and revisit them when necessary.

Have we written a good DPIA?

A good DPIA helps you to evidence that:

- you have considered the risks related to your intended processing; and
- you have met your broader data protection obligations.

This checklist will help ensure you have written a good DPIA.

We have:

☐ confirmed whether the DPIA is a review of pre-GDPR processing or covers intended processing, including timelines in either case;

☐ explained why we needed a DPIA, detailing the types of intended processing that made it a requirement;

☐ structured the document clearly, systematically and logically;

☐ written the DPIA in plain English, with a non-specialist audience in mind, explaining any technical terms and acronyms we have used;

☐ set out clearly the relationships between controllers, processors, data subjects and systems, using both text and data-flow diagrams where appropriate;

☐ ensured that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented;

☐ explicitly stated how we are complying with each of the Data Protection Principles under GDPR and clearly explained our lawful basis for processing (and special category conditions if relevant);

☐ explained how we plan to support the relevant information rights of our data subjects;

☐ identified all relevant risks to individuals' rights and freedoms, assessed their likelihood and severity, and detailed all relevant mitigations;

☐ explained sufficiently how any proposed mitigation reduces the identified risk in question;

☐ evidenced our consideration of any less risky alternatives to achieving the same purposes of the processing, and why we didn't choose them;

☐ given details of stakeholder consultation (e.g. data subjects, representative bodies) and included summaries of findings;

☐ attached any relevant additional documents we reference in our DPIA, e.g. Privacy Notices, consent documents;

☐ recorded the advice and recommendations of our DPO (where relevant) and ensured the DPIA is signed off by the appropriate people;

☐ agreed and documented a schedule for reviewing the DPIA regularly or when we change the nature, scope, context or purposes of the processing;

☐ consulted the ICO if there are residual high risks we cannot mitigate.

DPIA template

This template should be completed at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process.

It should be passed to the Data Protection Officer and Caldicott guardian for assessment once complete.

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA