Confidentiality Policy

Version Control

Date	Version Number	Stage	Author
16th September 2014	1.0	Creation	Tim Crowson
30th September 2014	2.0	Inclusion of revised access request form	Tim Crowson
29th October 2014	2.1	Review before presentation to Clinical Governance Group	Paul Haycox
5th November 2014	3.0	Additional comments from Sharon Leach	Paul Haycox
2nd December	4.0	Change of reference to Confidential waste policy	Tim Crowson
1st August 2016	4.1	Update of clinic identity	A Murdoch
26th August 2016	4.2	Minor changes and added reference to EU GDPR	P Haycox
30th December 2016	4.3	Addition of telephone recording information	A Murdoch
27th October 2017	4.4	No changes Required	A Murdoch
24th May 2018	5.0	Significant rewrite in relation to Data Protection Act. Included Requirements relating to role of Data Protection officer, individual's rights to access and rectify errors in records, revised access to records form, Data Protection Impact Assessments.	P Haycox
4th June 2021	5.1	National data opt out paragraph added	P Haycox

Contents

1. Introduction

Staff of St Michael's Clinic Ltd have access to a great deal of very sensitive and highly confidential personal information on a daily basis. The information is often patient specific and will include personal health details and other personal data. The confidentiality of this information must be respected and maintained at all times. All staff are therefore required to act in such a manner as to uphold the principle of confidentiality.

This policy will ensure that confidentiality is safeguarded and that all staff are aware of their responsibilities. The importance of this principle will be reinforced by inclusion in all job descriptions, training, induction programmes, appraisal processes and contracts of employment.

Breaches of confidentiality are likely to lead to disciplinary action for staff and/or the imposition of heavy fines on St Michael's Clinic Ltd if the Information Commissioner concludes the action "reckless". A health professional may be struck off their professional register as a result. A breach of confidentiality has the potential to damage the reputation, credibility, and good standing of St Michael's Clinic Ltd.

The policy applies to all St Michael's Clinic Ltd staff.

2. Background Information

This policy reflects a number of Acts, Codes of Practice and responsibilities:

> **The General Data Protection Regulation (GDPR).** The GDPR is a European Law, which is enshrined in English Law alongside the Data Protection Act 2018. It lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. It also enshrines the legal basis upon which data can be processed and the individual's right to transparency in data processing and their rights to review and challenge data held by organisations

The Data Protection Act 2018 (DPA). The DPA supplements the GDPR and gives legal rights to the Information Commissioners office as the regulator. It defines the UK law in certain areas on the processing of data.

Human Rights Act 1998. This Act was passed as a result of the European Convention on Human Rights. This is intended to protect certain rights of individuals. In terms of Confidentiality, the key part is Article 8; "the right to respect for private and family life, home and correspondence". This gives an individual the right to live their life with personal privacy in a way that does not infringe on the rights of anyone else. This could include information held about them in the form of diaries or personal records and correspondence aspect is equally as broad.

The Health & Social Care Act 2001 (section 60). This section gives the Secretary of State, powers to permit the use of patient data in certain special cases without the necessity of gaining consent. An example of these powers has been to allow disclosure of patient data to support activities for cancer registries. It is this section that will usually apply to nationally managed research activity.

Freedom of Information Act 2000. This Act is part of the Government's commitment to make more public sector information available to the public. It does however outline several exemptions to protect certain information which includes patient identifiable information. For more information see the Freedom of Information Policy.

Regulation of Investigatory Powers Act 2000. This Act is intended to combat cybercrime. It ensures that any interceptions do not breach an individual's human rights and requires that appropriate authorisations are obtained when required. The Act also supplements existing legislation, for example, any information collected under this Act still falls under the Data Protection Act and its principles.

Information Governance. Provides a framework to bring together all the requirements, standards and best practice that apply to the handling of personal information. One of the aims is to support the provision of high quality care by promoting the effective and appropriate use of information.

Caldicott Reviews. The 1997 review of the uses of patient identifiable information by Dame Fiona Caldicott devised six general principles of information governance that could be used by all NHS organisations with access to patient information. The further Information Governance Review in March 2013 set out 26 recommendations to improve information governance nationally and after the 2020 review another principle was added.

GENERAL MEDICAL COUNCIL; Confidentiality: Good practice in handling patient information.2018

3. Responsibilities

Business Owner

The Business Owner has overall responsibility for ensuring that the Clinic meets its statutory responsibilities, however day to day responsibility is devolved as set out below.

Data Controller

The data controller has overall accountability for establishing and maintaining a safe and effective data management system that adheres to all statutory and regulatory guidelines. Our Data Controller is Dr. Stephen Murdoch.

Caldicott Guardian

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. Our Caldicott Guardian is Dr. Stephen Murdoch.

Senior Information Risk Owner (SIRO)

The SIRO is responsible for identifying and managing the information risks to the organisation and its business partners. This will include oversight of the organisation's information security incident reporting and response arrangements. Our SIRO is Mr. Paul Haycox.

Data Protection Officer (DPO)

The Data Protection Officer will be responsible for monitoring compliance of the clinic against the GDPR. Specifically they will be responsible for:-

- Advising management and staff on their obligations in relation to the GDPR
- Monitor compliance with the GDPR in relation to policies, processes and staff awareness
- Advise on the requirement for, and completion of, Data Protection Impact Assessments
- To be first point of contact for Data Access Requests
- To be first point of contact for the Information Commissioners Office

Our Data Protection Officer is Mrs. Amanda Copeland.

All Managers

All Managers are responsible for ensuring that all Clinic imperatives, relating to confidentiality issues, are acted upon by their staff. Additionally, managers are responsible for:

Assessing, and reporting as necessary, on any confidentiality risks in their areas.

Ensuring that staff complete risk event forms for all confidentiality breaches.

Ensuring that all patient data is secure in their areas and that "safe haven" procedures are in place particularly in relation to patient records and fax machines.

Staff

All Staff are responsible for:

Making themselves aware and fully understand their legal obligation to keep personal information obtained through their work confidential.

Participating in induction, training and awareness raising sessions carried out to inform/update staff on confidentiality issues.

Challenging and verifying where necessary, the identity of any person who is making a request for confidential information and to determine the validity of their reason for requiring that information.

Reporting any actual or suspected breaches of confidentiality to their line manager.

4. Uses and Disclosure of Patient Health Data

All processing of data must be lawful. The clinic has mapped data flows and noted the legal basis for each data set being held and processed. The main patient facing basis are:

Article 6 of the GDPR outlines the lawful basis upon which personal data can be processed. Article 9 outlines the legal basis for processing of special categories of personal data.

The legal basis for processing NHS patient data under Article 6 of the GDPR 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 legal basis for processing private patient data under Article 6 of the GDPR is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract

The legal basis for processing NHS data under article 9 is necessary to protect the vital interests of the data subject

The legal basis for processing private patient data under article 9 is necessary to protect the vital interests of the data subject

There are a number of other times at which data has to be shared and these are laid out in articles 6 and 9 and can be expanded upon by the Data Protection officer.

Only persons who are directly involved in the above and have legal right to view the data can have access. In all cases the minimum amount of information should be disclosed and accessed.

Where it is possible to do so, data must be anonymised or pseudonymised.

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.

Where patient information is being accessed for research or education, each access will require explicit and informed patient consent unless the research is being managed centrally and the Health & Social Care Act 2001 (section 60) applies.

5. Guidelines to be followed

Personal Information

Personal information may relate to patients, members of staff, visitors, carers and other members of the public. To ensure the confidentiality of personal information, the following must be adhered to:

Information must be kept up to date and accurate. Checks to maintain accuracy when patients attend appointments will be made. Any inaccuracies will be noted and amended.

Any records that are found to have inaccurate information in them (such as incorrectly filed photographs or reports) will be immediately corrected upon identification and noted in the record.

Access to areas, departments or offices containing confidential information must be restricted to authorised personnel only.

Information of a personal nature must not be left unattended in a public area, this includes patient records, faxes, and telephone messages.

Staff must not access any patient, employee of other record for which they have no proper reason to do so in the course of their duties within St Michael's Clinic Ltd.

Staff must never access patient records for their personal interest (this includes their own health records or those of another staff member).

Compliance with all the relevant IT policies that exist to keep information secure.

Corporate Information

Staff must ensure that corporate/business information is only viewed by those who need to see in line with their role.

6. Staff Resignation

When a member of staff leaves their former manager must ensure that:

Rights of access to computer systems are rescinded.

Identity badges are returned.

All St Michael's Clinic Ltd keys are returned.

7. Transporting and Moving Information Around

Manual and electronic confidential information must always be transported in a manner that ensures that it is not lost or accidentally disclosed to unauthorised individuals:-

All laptops will be password protected. Any personal data must be held on encrypted memory sticks (Kingston DataTraveler Locker+ G3 have been made available to key personnel)

If staff must transport patient records in their own cars, then the records must be locked in the car boot and the car must never be left unattended. Staff should not take records home with them (this includes medical staff).

Staff taking non-patient identifiable work home with them are responsible for ensuring that the information remains safe and is not viewed by anyone not associated by St Michael's Clinic Ltd (including family members).

The routine transportation of notes and specimens should be through the non-patient transport system.

8. Informing People on the Use of their Information

The GDPR makes it clear that personal data should be processed in a transparent manner.

The clinic has a Privacy Notice (attached as Appendix 1) that outlines

The type of data collected

The purpose for which it is being used.

Other parties that it may be shared with.

Security measures applied.

The rights of the individual

The Privacy notice is referenced in all letters for new appointments, is available on line at the clinics website and is displayed in the waiting area.

No individual's identifiable information will be used without explicit consent for audit and research purposes.

Patients have the right to be informed how their information is used and to record their consent, dissent and objections.

Patients may also contact St Michael's Clinic Ltd about a number of issues related to the use of their personal information which may include requests for certain disclosures of their information to be restricted. A good example of this is requests by patients not to have their summary health record available on the national "spine" of EMIS. The individuals' wishes would be respected unless there are exceptional circumstances.

All staff who receive communications from patients about disclosures of their records or are considering new uses or disclosures of records must first contact the Business Manager, IT manager or the Caldicott Guardian to ensure appropriate action is taken.

9. Information Sharing with other Agencies who are not IG toolkit compliant

It will be necessary for essential personal information to pass between St Michael's Clinic Ltd and other NHS services. This may happen where one of these services is contributing towards a programme of care.

In any cases of "routine" data sharing, where the sharing is not associated with direct patient care and the bodies are not compliant with the Information Governance Toolkit, then all parties involved in the data sharing should set up a data sharing protocol.

All personal information that is used in the protocol must meet the conditions for processing as laid down in the GDPR and Data Protection Act 2018 and the Caldicott review recommendations. If the information is to be shared for a different purpose to that for which it was given, it should only be disclosed if a

legal basis for sharing can be established under Article 6 and Article 9 of the GDPR.

Each case will be judged on its merits as to whether a disclosure without consent is justified.

Information which has been aggregated and/or anonymised, can generally be shared for justified purposes. Care must be taken that an individual cannot be identified from this type of information as it can be possible to identify individuals from limited data e.g. numbers of patients suffering from a very rare health condition.

10. Disclosure of Personal Information to the Police

When St Michael's Clinic Ltd receives a request for personal information from the Police, certain information can be released under the following conditions:

The police have produced a court order.

The information is required under the Road Traffic Act.

The information is subject to an Exemption under the Data Protection Act, usually S.29 Crime and Taxation.

The request is made to meet the requirements of the Crime and Disorder Act 1998 e.g. where the police can provide evidence that disclosure will assist the police in prosecuting serious crime such as murder or rape.

Information can also include any CCTV footage retained by St Michael's Clinic Ltd.

Any requests to St Michael's Clinic Ltd by the Police will be managed by the Business Manager or the IT Manager, in discussion with the Caldicott Guardian. No other member of staff is authorised to approve this disclosure.

11. Access to Health Records

Medical Records do not belong to the patient, but patients have a right under the GDPR to request access to the records that St Michael's Clinic Ltd holds on them. This can involve St Michael's Clinic Ltd providing them with either manual or electronic copies or in some cases arranging for the patient to view their records.

When requesting access to their own records, no unnecessary barriers should be placed in front of the individual.

The request can be made in person, by letter or by e mail. All requests should be sent to the Data Protection Officer.

If the patient is known to the clinic and identity is not in question, then no additional identification is needed. However, if identification is not certain, then photo identification will be required.

The request should provide enough proof to satisfy the clinic of their identity. Where requests are made on behalf of the individual patient, the clinic must be satisfied that the individual has given consent to the release of their information.

It would be helpful if the form at Appendix B is completed and signed by both the requesting party and the authorising clinic officer. However, this is not mandatory, and the patient has the right to refuse.

At all times, the request should be logged on receipt. A note of the exact information shared must be made in the patients record – along with the date and mode by which it was sent. This should also be logged with reception onto the Data Access Request log.

The data must be supplied within 28 days of receipt of

No charges can be made for copies of records, unless further requests are made that are considered excessive in their nature.

If the records contain information supplied by a third party who clearly would not have provided the information had they thought that their contribution would be disclosed, then the name of the contributor and their information should not be supplied to the data subject and the information redacted.

In the event that St Michael's Clinic Ltd receives a request from a patient who has suffered significant trauma, e.g. major accident disfigurement or serious burn, the treating clinicians will be informed of the request to ensure that disclosure is in the best interests of the patients particularly as the records are likely to contain distressing clinical photography. The treating consultant or a member of their team will supervise these disclosures or partial disclosures. However, the purpose of this is to disclose as much as possible not to prevent legal access and to achieve this as safely as possible and act at all times in the best interests of the patient.

St Michael's Clinic Ltd will not manage the records of the deceased differently than it manages the records of the living.

12. Requests to correct errors in, or delete, records

Any requests from data subjects to amend or erase records that are brought to the attention of the clinic will be reviewed by the Data Protection Officer and the Caldicott Guardian within 14 days of the matter being raised. The request must be in writing (an e mail is sufficient).

Any amendments to records will be considered against the requirements of the General Data Protection Regulation and the Data Protection Act 2018 – alongside the legal requirements relating to medical records.

The data protection officer will write to the data subject with a decision regarding the request – this will include consideration of correcting the record if inaccurate, , rectifying it and/or erasure (subject to the outcome of the review and the reason the data is held).

13. Requests to restrict or cease processing of data

At the request of an individual, made in writing, the Data Protection Officer will review any request to restrict or cease the processing of personal data. The Data Protection Officer will respond to the request within 28 days of receipt.

14. Telephones, Answering Machines, Faxes and Overheard Conversations

Telephone Enquiries. Always be sure that the caller is who they say they are, unless it can be verified beyond doubt, do not give patient identifiable information.

Telephone conversations may be recorded if that call is deemed to be of a such a nature that review of the conversation may be required. Notice that calls may be recorded is provided as part of the recorded message for all telephone calls.

Answering Machines. Staff may only leave a message on a patient's home landline if it is absolutely necessary and then leave name and number. Ideally permission will have been obtained from the patient to leave messages on a home landline. It is better to use answering machine function on mobile phones as more detailed information can be left as there is a reduced risk that uninvolved others can access the call details.

Email. Patient identifiable information should never be included in the main body of an email, unless password protected using an accredited software package – such as Winzip, Ironport, etc or using nhs.net to nhs.net e mail accounts. If password protected, then the password must be agreed with the recipient in advance of sending.

Fax machines. All faxes must be sent to a safe location where only staff who have legitimate right to view the data can access it. The sender must be certain the correct person will receive it. Care must be taken dialling the right number; setting up simple number codes for routine faxes will help.

Overheard Conversation. Where conversations are conducted by staff relating to St Michael's Clinic Ltd business either over the phone, face to face, or in the close proximity of public or reception areas, then care must be taken that person identifiable information is not overheard by persons who do not have a right or need to hear such information.

15. Confidential Waste

All paper that contains sensitive patient or Clinic information must be disposed of in line with the Document, Record and Lifecycle Management Policy and Credit Card Policy.

16. Training

Training in information governance, which includes confidentiality, is mandatory for all staff.

17. Data Protection Impact Assessments (DPIA)

A data protection impact assessment will be undertaken on any project that will have a significant impact on how data is processed. That could be as a result of:-

- Implementation of new technologies
- Any change in processing that could be considered "high risk" for the individuals data i.e. change in the level of processing, the type of processing, a third party processor becoming involved or if a processor starts to use services in a non-EU country

The Data Protection officer will be informed and support the DPIA.

The project should not commence until the DPIA has been signed off by the DPO and Caldicott Guardian

Appendix 3 gives a template for the DPIA

Appendix 1

Privacy Notice

We collect personal data from you when you are referred to our clinic or use our services. We will always aim to keep this data secure and use it only for the purposes that we are legally allowed.

For example, we collect and store information that we receive from your GP and other health professionals when you are sent to us for care. We will also gather information from you at your appointments and may request historic information from other health clinics of past health episodes if these are relevant to the care we are providing you. Some of the information we hold we recognise will be sensitive.

The information we hold will include contact details (name, address, telephone numbers, e-mail), personal details (gender, date of birth, GP practice, emergency contacts) and medical information. We may also take and store photos of your skin complaint.

We use this information and medical records primarily to ensure the safe and effective delivery of care. Parts of the records will be used for the efficient management of the NHS; to undertake medical audits that improve our overall care for patients and occasionally in medical research. We will also use your mobile phone number to send you appointment reminders.

Who else has access to your data

At times, we do need to share information with other health service bodies, to ensure you receive the best care from us and the health service generally, and so that we can administer the service. We will only send the minimum level of information that is necessary in these cases.

We do employ the services of other organisations who will process your data on our behalf – particularly our computer system providers. These companies will not use your data in anyway outside of this privacy policy and we are ensuring we have agreements in place that makes this clear.

We also need to comply with the any legal requests for information from public bodies – such as the police and government bodies – or to protect you, ourselves and others.

Your rights over your data

You have the right to be informed how we use your data. If you have any queries over and above the contents of this policy then please contact our data protection officer, Mr Paul Haycox, on dpo@stmichaelsclinic.co.uk

You can also request a summary of the information that we hold on you or for us to correct any factual data that is inaccurate. The first request for information will be provided free of charge, but a charge of £10 may be charged for subsequent requests, if they are felt to be excessive.

You may ask us to delete information that we hold on you, which we will consider. However, it is a legal requirement to maintain medical records for a defined period of time (we abide to the current retention schedules contained in the "Records Management Code of Practice for Health and Social Care 2016") and so these will be considered alongside any request.

To make a request for any of the above, please email us at dpo@stmichaelclinic.co.uk

Finally, if you are unhappy with how we are managing your personal data, or aren't happy with our response at any time, then you have the right to file a complaint with the Information Commissioner's Office

Security

We use reasonable and modern methods to protect your data, but unfortunately no data transmission or storage system is 100% secure. If you feel that the security of your information has been compromised in anyway then please contact us immediately. If we become aware of any security issue, then we will contact any individuals that are affected.

How the NHS and care services use your information

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is only used like this where allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

See what is meant by confidential patient information

Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care

Find out more about the benefits of sharing data

Understand more about who uses the data

Find out how your data is protected

Be able to access the system to view, set or change your opt-out setting

Find the contact telephone number if you want to know any more or to set/change your opt-out by phone

See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and

https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

The legal conditions for processing personal data is public interest or in exercise of official authority and contractual necessity. The legal condition for processing special categories of personal data are Health and Social care or vital interests.

This privacy policy was last updated on 3rd June 2021

Appendix 2

Dr Stephen Murdoch MB ChB FRCP
GMC Number 3354458
Consultant Dermatologist

St Michael's Clinic Ltd
St Michael's Street
Shrewsbury
Shropshire SY1 2HE

Enquiries: 01743 590010
Fax: 01743 590017

Email: Info@shropshireskinclinic.co.uk

Access to Health Records under the General Data Protection Regulation (Subject Access Request)

It is not mandatory to complete this form, but it will help us administratively

I am applying for access to view my health records:

FULL NAME	
DATE OF BIRTH	
ADDRESS	
CONTACT NUMBER	

You do not have to give a reason for applying for access to your health records. However, to help us save time and resources, it would be helpful if you could provide details below, informing us of periods and parts of your health records you require, along with details which you may feel have relevance i.e. consultant name, location, written diagnosis and reports etc.

DATE AND TYPES OF RECORDS:	

IN CASES WHERE IDENTIFICATION IS UNCERTAIN WE REQUIRE PHOTO ID

Dr Stephen Murdoch MB ChB FRCP
GMC Number 3354458
Consultant Dermatologist

St Michael's Clinic Ltd
St Michael's Street
Shrewsbury
Shropshire SY1 2HE

Enquiries: 01743 590010
Fax: 01743 590017

Email: info@shropshireskinclinic.co.uk
Web: www.shropshireskinclinic.co.uk

Access to Health Records under the General Data Protection Regulation (Subject Access Request)

It is not mandatory to complete this form, but it will help us administratively

PRINT NAME:	
SIGNED:	
DATE:	

……

OFFICE USE ONLY

RECEIVED BY:	
SIGNED:	
DATE:	

IN CASES WHERE IDENTIFICATION IS UNCERTAIN WE REQUIRE PHOTO ID

Appendix 3

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