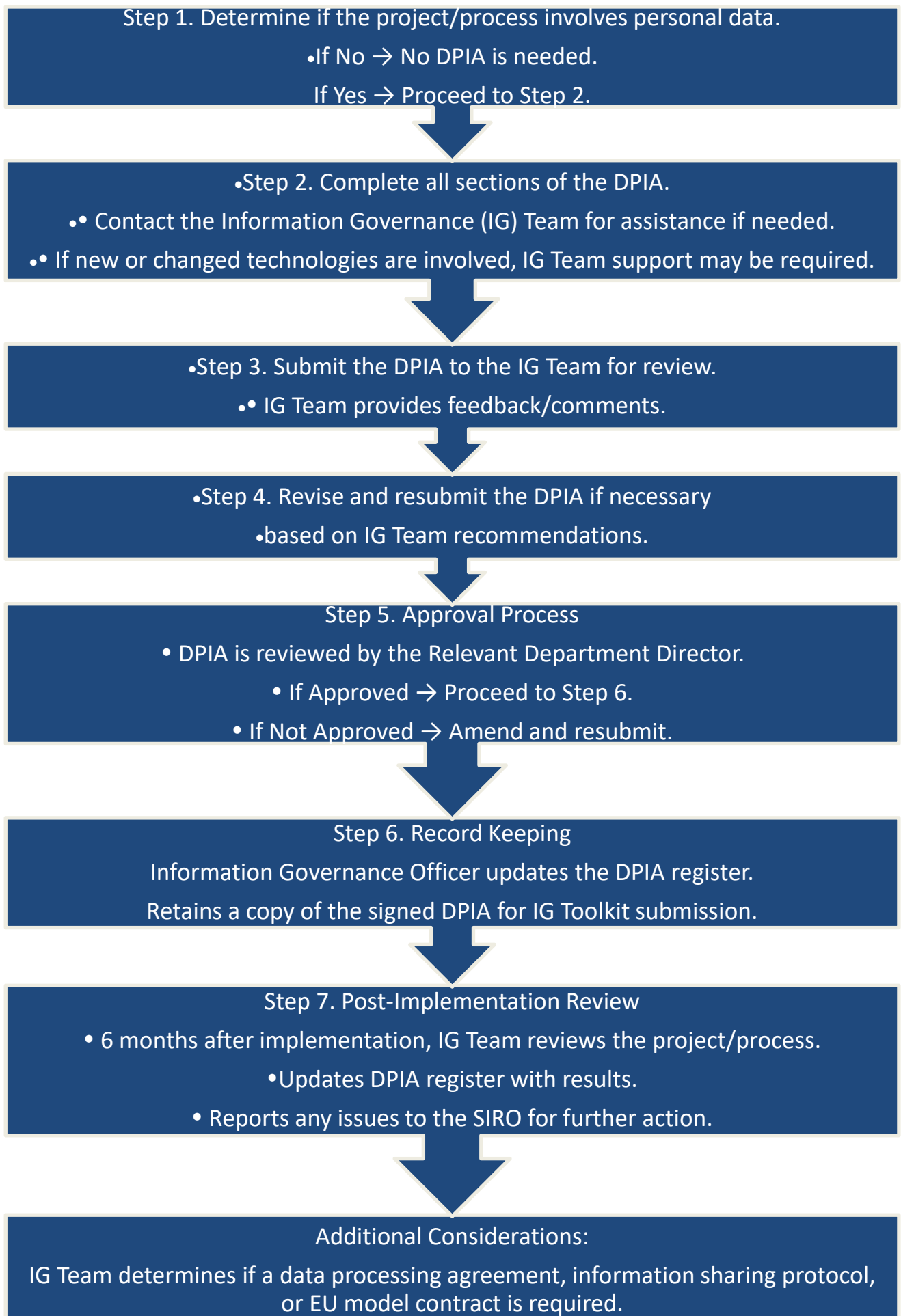


DATA PROTECTION IMPACT ASSESSMENT

Classification <i>To be completed by the IG team</i>	OFFICIAL
Project title	South Bank Close and Ivy Close lease surrender, and provider procurement – Concept
Version	0.02
Updated	
Date	13.08.26

THIS IS A LIVE DOCUMENT AND SHOULD BE REVIEWED AND UPDATED THROUGH THE LIFE OF THE PROJECT.

- The Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.
- This document must be completed for any new project/process or change in current process which will either involve a new use of personal data or will significantly change the way in which personal data is handled.
- It must be completed as soon as the new process or change in process is identified by the Project Manager or Information Asset Owner.
- Please refer to **Appendix A** for additional guidance on when to complete a DPIA.



PROCESS

Please complete Sections **A & B** as fully as possible.

If the project involves the procurement of a new or replacement system/service from a third-party supplier, it will not be possible to answer all questions in **Section B** during the early stages of the project. However, this information should be requested from suppliers during the procurement process and the DPIA will need to be updated once the preferred supplier is known.

Once this DPIA has been completed please email to:

InformationGovernance@herefordshire.gov.uk

The IG Team will complete Section C and return for you to obtain your Director's approval.

Once approved, please send a copy of the approved and signed DPIA to the IG Team for our records.

TO BE COMPLETED BY SERVICE AREA**SECTION A) DETAILS OF NEW OR CHANGES PROJECT/PROCESS****1) Project title**

South Bank Close and Ivy Close lease surrender, and provider procurement.

2) Project purpose

- Explain broadly what the project aims to achieve
- What types of data will be processed?

For example, A new cloud-based Human Resources Information System (HRIS) to manage staff data. This system will centralise employee records, including personal details, job roles, performance reviews, training history, and absence management. It will also integrate with payroll and benefits platforms.

This project involves:

- Large-scale processing of personal data, including sensitive information such as health-related absence records.
- Use of cloud services, which introduces risks related to data transfer, storage, and third-party access.
- Automated decision-making, such as flagging performance issues or triggering absence alerts.
- Remote access and mobile use, increasing the risk of unauthorised access or data breaches.

South Bank Close and Ivy Close are residential properties in Hereford, that function as supported living facilities for adults with disabilities or special care needs.

Herefordshire Council owns the South Bank and Ivy Close properties in Hereford.

The properties are currently subject to lease arrangements with Midland Heart. Midland Heart lease the buildings and provide building management.

Midland Heart has requested to surrender its leasehold interest because the properties are geographically distant from its operating area and no longer align with its core business priorities.

As an interim measure Midland Heart have engaged Stonewater Ltd to undertake the housing management of these units of accommodation.

The Council must now manage the surrender of Midland Heart's leasehold interest at South Bank and Ivy Close and procure a new long lease holder who will provide housing management .

Data will need to be exchanged between Midlands Heart, Stonewater and the new lease holder to ensure the safety of existing residents.

Care and support is provided to residents by Aspire (at the moment) via a separate set of contractual arrangements, but they too may need to share data with the new lease holder for housing management and safety purposes.

The Council have nominations to these properties so will also exchange personal data with the new lease holder for housing management and safety purposes.

Throughout this process the Council aims to maintain continuity and stability for residents, protect the Council's property interests, and ensure the schemes continue to provide appropriate accommodation for vulnerable adults.

3) Assessment complete by**Name**

Hannah McSherry

Job title

Strategic Housing Manager

Team

Strategic Housing

Directorate

Community Wellbeing

Phone number

01432 383531

Email Address

Hannah.mcsherry2@herefordshire.gov.uk

4) Information Asset Owner e.g. Service Director / Service Manager

Name	Hayley Crane	
Job title	Head of Housing	
Team	Housing Service	
Directorate	Community Wellbeing	
Phone number	01432 261919	
Email Address	Hayley.crane@herefordshire.gov.uk	
5) For personal data being processed please indicate the status of Herefordshire Council	Data Controller The Data Controller makes decisions about processing activities. They exercise overall control of the personal data being processed and are ultimately in charge of and responsible for the processing.	☐
	Joint Data Controller Joint Data Controllers together decide the purposes and means of processing personal data. They collaboratively determine how and why personal data is processed and share responsibility for complying with data protection laws.	☐
	Independent Data Controller Where more than one organisation makes decisions about processing activities for their organisation. They exercise overall control of the personal data being processed by them and are ultimately in charge of and responsible for the processing.	☒

SECTION B) DATA PROTECTION IMPACT ASSESSMENT QUESTIONS

6) Will the new (or amended) process contain personal identifiable data? If yes, in relation to who?	No <u>If 'no' you do not need to complete any further information as a DPIA is not required.</u>	☐
	Service Users	☒
	Staff	☐
	Other (please specify) We have contacted Midlands Heart and Stonewater who are currently undertaking housing management at these properties	

		to ensure that there are no TUPE implications. If they come back and say there are TUPE implications, I will update this.			
7) Please tick the data items that are held in the system or involved in the process					
Personal Information					
Name	☒	Address	☒	Postcode	☒
Date of Birth	☒	Sex	☒	Next of Kin	☒
GP	☒	NHS number	☐	National insurance number	☒
Other (please specify)					
To be updated once more info available.					
Special Category (Personal Information)					
Ethnic Origin	☒	Genetic/Biometrics	☐	Union membership	☐
Physical or Mental Health	☒	Political Opinions	☐	Religion	☐
Sexual Orientation	☐	Other (please specify) Limited physical / mental health details for site safety requirements.			
8) Legal Basis for Processing Have you established which article 6 conditions (legal basis) for processing apply? (the conditions can be found)		(a) Consent the individual has given clear consent for you to process their personal data for a specific purpose. (if yes, see questions 11 and 12)			☐
		(b) Contract the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering a contract.			☒

	(c) Legal obligation the processing is necessary for you to comply with the law (not including contractual obligations).	☐
	(d) Vital interests in the processing is necessary to protect someone's life.	☐
	(e) Public task the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.	☒
9) Legal Basis for Processing If special category data is involved have you established which article 9 conditions (legal basis) for processing apply?	(a) Explicit consent The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject. (if yes, see questions 11 and 12)	☐
	(b) Employment, Social Security and Social Protection Law Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;	☐
	(c) Vital interests Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;	☐
	(d) Not-for-profit bodies Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the	☐

	personal data are not disclosed outside that body without the consent of the data subjects;	
	(e) Made public by the data subject Processing relates to personal data which are manifestly made public by the data subject;	☐
	(f) Legal claims and judicial acts Processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity;	☐
	(g) Substantial public interest conditions Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;	☐
	(h) Health or 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;	☒
	(i) Public health Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;	☐
	(j) Archiving, research and statistics Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law	☐

	which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.	
10) Is a third party supplying the new system or process?	Yes	☒
	No	☐
11) Who provides the information?	Data Subject	☒
	Staff	☒
	Other (such as police, NHS, GP etc. please specify)	☒
12) If you are relying on consent to process personal data, how will this be obtained and recorded?	N/A	
13) If the data subject withdraws their consent how will this be actioned and recorded?	N/A	
14) Do you have a Council Privacy Notice that covers the collection and processing of this data?	Yes (please attach a copy) Would it fall under the wider ASC privacy notice that covers housing as well? Adults' wellbeing privacy notice - Herefordshire Council	☒
	No	☐
15) What measures are in place / are you putting in place to ensure that the information is secure?	A data sharing agreement will be needed for all parties to ensure there is a clear exchange of information for the new lease holder. Specifically between Midlands Heart, Stonewater and the new leaseholder. A separate data sharing agreement may also be needed between the care and support provider and the lease holder	

16) Are any decisions made by automated decision making processes/AI with this system/project? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Yes	☐
	Please provide details of the types of decision and how individuals are notified.	
	No	☐
17) Who will have access to the Information? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Subject to tender process (to be updated once supplier has been identified)	☒
	Council	☐
	Processor	☐
	Other (please provide details)	☐
18) Is there an audit trail in place for the system to identify who has amended a record? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Subject to tender process (to be updated once supplier has been identified)	☒
	Yes If yes, please provide details	☐
	No	☐
	Subject to tender process (to be updated once supplier has been identified)	☒
19) Is there an audit trail to identify who has accessed a record? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Yes If yes, please provide details	☐
	No	☐
	Subject to tender process (to be updated once supplier has been identified)	☒
20) What training and/or guidance is in place to ensure that staff know how to operate the system access and process the data securely?	Herefordshire Council has a comprehensive approach to data management and mandatory training.	

		Provider will need to demonstrate comprehensive information governance training, process and procedures as part of procurement process.			
21) What are the council retention periods for this data and are these documented? Retention schedules can be found here: Retention Schedules		The Council retention periods will apply to data we own, but may differ from third party providers. This section will need to be updated following the tender process.			
22) Please state how the data will be sent/accessed					
By courier	☐	By post – internal	☐	Secure file transfer	☒
By hand	☐	By post - external	☐	Email (secure network)	☒
By telephone	☐	Website	☒	Email (unsecure network)	☐
Secure portal	☐	Other (please specify) This needs to be confirmed by the provider(s) discussed in this DPIA including the new lease holder.			
23) If a third-party data processor is to be used, confirm that a data processing agreement will be completed? The council's standard contract templates all contain a data processing agreement. If you are not using a council template, please check with Legal Services (PracticeManagement@herefordshire.gov.uk) before proceeding.		Yes			☐
		N/A not a third party			☐
		No If no, contact the IG Team for further information InformationGovernance@herefordshire.gov.uk			☐
24) Will the process be transferring any personal and/ or sensitive data to a country or countries		Yes If yes, please list the country or countries:			☐

outside of the EEA (European Economic Area)? If undergoing a tender process for a third-party supplier, choose “Permitted” if there is a chance that the successful supplier will be transferring Data outside of the EEA. For example, this might be because you are not including any restrictions on the transfer of data in your tender/contract documents, or due to the nature of the system/service it is necessary or common practice for suppliers in that market to transfer data outside of the EEA. This may need to be updated once the supplier has been identified.		
	No	☒
	Permitted [Insert reasoning]	☐
25) Please specify what types of data will be transferred to the non EEA country or countries? If undergoing a tender process for a third party supplier this may need to be completed once the supplier has been identified.	N/A	
26) Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country or countries? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Yes, please specify those measures	☐
	No	☐
	Subject to tender process (to be updated once supplier has been identified)	☐
28) Have you checked whether the non-EEA country has an adequate level of protection for data security? If undergoing a tender process for a third party supplier this may need to be completed once the supplier has been identified.	Yes Please provide evidence of this	☐
	N/A	☐
	No	☐

	Subject to tender process (to be updated once supplier has been identified)	☐
27) Will the data be shared with any other parties (other than those providing the system)? If undergoing a tender process for a third-party supplier this may need to be completed once the supplier has been identified.	Yes, If yes, please provide details of who/where it is being sent to (including any external organisations) Data will be exchanged with the care and support provider and as part of the handover between leaseholders.	☒
	No	☐
	Subject to tender process (to be updated once supplier has been identified)	☐
29) Is there a council contingency plan/business continuity plan or backup policy in place to manage the effect of an unforeseen event?	Yes, please provide link here	☐
	No – not that I am currently aware of.	☐
30) Has the third party / supplier of the system registered with the Information Commissioner? (this is available at Information Commissioner's Office - Register of data protection fee payers (ico.org.uk))	Yes, ICO Registration Number is....	☐
	No	☐
	Subject to tender process (to be updated once supplier has been identified)	☒
31) What level of info/cyber security assurance is required from the third-party supplier? Your response to this question will determine the type and level of assurances that need to be provided by suppliers during a procurement process. <i>See appendix B.</i> If you are unsure which option is right for your project, please contact: InformationGovernance@herefordshire.gov.uk	N/A (no third-party supplier)	☐
	(A) Minimal For the lowest risk contracts, where very limited personal data will be processed and there is a low risk of harm in the event of a data breach. The following <i>could</i> indicate that a 'minimal' level of assurance is required: - You responded "No" to Question 24 (if data would be transferred outside of the EEA); and - You did not tick any of the boxes for Special Category Data under Question 7; and	☐

	- The system/process impacts only a limited group of data subjects; and - You ticked only one or two boxes under 'Personal Information' for Question 7 (e.g. Name and Date of Birth).	
	(B) Low For contracts where there is a moderate quantity of personal data being processed, but a low risk of harm in the event of a data breach. The following <i>could</i> indicate that a 'low' level of assurance is required: - You responded "No" to Question 24 (if data would be transferred outside of the EEA); and - You did not tick any of the boxes for Special Category Data under Question 7; and - The system/process impacts a wider group of data subjects; and - You ticked only one or two boxes under 'Personal Information' for Question 7 (e.g. Name and Date of Birth).	☐
	(C) Medium For contracts involving significant levels of personal data and/or some special category data, and where there is a moderate risk of harm in the event of a data breach. The following <i>could</i> indicate that a 'medium' level of assurance is required: - You responded "No" to Question 24 (if data would be transferred outside of the EEA); and - You ticked one or more boxes for Special Category Data under Question 7; or - You ticked many boxes under 'Personal Information' for Question 7 (e.g. Name, Date of Birth, sex, Address, NIN); or - The system/process impacts a large group of data subjects.	☒
	(D) High For higher-risk contracts, involving significant levels of personal data and/or special category data	☐

	The following <i>could</i> indicate that a ‘high’ level of assurance is required: • You responded “Yes” or “Permitted” to Question 24 (if data would be transferred outside of the EEA); or • The system/process impacts a large group of data subjects; and ○ You ticked numerous boxes under ‘Personal Information’ for Question 7 (e.g. Name, Date of Birth, sex, Address); or ○ You ticked one or more boxes for Special Category Data under Question 7.	
--	---	--

FOR COMPLETION BY THE IG TEAM - SECTION C – RISK ASSESSMENT

The following risks should be referred to as a checklist

Risk that processing is not transparent, lawful or that not all purposes for processing are covered

Risk that current processing is not compatible with new purposes if using existing personal data

Risk that inadequate data quality means the information is not fit for the identified purpose(s)

Risk that any data matching or linking may link the wrong records together

Risk that information is kept for too long or for not long enough or not securely destroyed

Risk that personal data will be lost, damaged or otherwise put at risk by inadequate security controls

Risk that data will be shared or accessed inappropriately

Risk that those handling the data are not aware of their data responsibilities

Risk to individual’s right of access, rectification, erasure, and object to or restrict processing

Risk from information being outside the UK

Risk if financial loss / fraud for individuals

	Minimal	Significant	Severe
Remote	LOW	MEDIUM	MEDIUM
Possible	LOW	MEDIUM	HIGH
Probable	MEDIUM	HIGH	HIGH

Privacy Risk/Issue	Likelihood of harm	Severity of Harm	Overall Risk	Solutions/Mitigations
Risk that processing is not transparent, lawful or that not all purposes for processing are covered	Remote	Significant	Medium	Care Act requirements to be reviewed as project to procurement new service is undertaken. Amendments and notification made as necessary.

	Name, position and date	Comments or actions identified
Measures approved by		
Residual risks approved by		

Any actions identified should be linked to the project plan and monitored for completion.

IG Sign off by (name & position)	SIGN OFF FOR CONCEPT DPIA 13/08/26 V0.02 ONLY Sam Smith Information Governance and Data Protection Officer	Date	13/08/26
---	--	-------------	----------

Director Approval	
Name	
Job Title	
Signature	
Date Approved	
Comments	
Updates approved date	

Appendix A

Aim

The aim of this guidance is to ensure all staff understand what a Data Protection Impact Assessment (DPIA) is and when one needs to be completed.

What is a Data Protection Impact Assessment and When should one be completed?

The function of the DPIA is to ensure that data protection risks are properly identified, recorded and addressed at an early stage wherever possible, and that decision-makers have been fully informed of the risks and the options available for mitigating them.

The DPIA must be completed as soon as the new project, service, or change is identified by the Project Manager / System Manager or Information Asset Owner.

The DPIA should be completed by someone involved in the project that can answer all the questions with authority.

The live document should be reviewed and updated during the life of the project.

What do I have to complete?

You need to complete the Data Protection Impact Assessment Document available on the intranet considering the risks listed above. Please be aware that we have a legal responsibility to publish details of Data Protection Impact Assessments completed by the organisation. Please consider whether any information contained within the assessment document will be commercially or confidentially sensitive.

What risks need to be considered ?

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisation's to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification

or the disclosure of information.

- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary

Corporate Risks

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation

Reducing the risks

There are many different steps which organisations can take to reduce a privacy risk. Some of the more likely measures include:

- Deciding not to collect or store particular types of information.
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information.
- Implementing appropriate technological security measures.
- Ensuring that staff are properly trained and are aware of potential privacy risks.
- Developing ways to safely anonymise the information when it is possible to do so.
- Producing guidance for staff on how to use new systems and how to share data if appropriate.
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests.
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the organisation for assistance if necessary.
- **Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed**

on an organisation's behalf and Data Processing agreement.

- Producing data sharing agreements which make clear what information will be shared, how it will be shared and who it will be shared with. (not relevant to processors)

Organisations will need to assess the costs and benefits of possible privacy solutions. Some costs will be financial, for example an organisation might need to purchase additional software to give greater control over data access and retention. The costs can be balanced against the benefits, for example the increased assurance against a data breach, and the reduced risk of regulatory action and reputational damage.

What should I do next?

The completed document must be emailed to
InformationGovernance@herefordshire.gov.uk

Appendix B

What level of info/cyber security is required?

These categories align with the procurement process – this is the information that will be requested from providers and will be assessed during the tender process, based on the risk classification that you have determined by completing this DPIA:

Option A – Minimal

This should be selected for the lowest risk contracts where there is very limited personal data that will be processed.

GDPR

Please confirm that you have in place, or that you will have in place by the award of the contract, the human and technical resources to perform the contract to ensure compliance with the UK General Data Protection Regulation and to ensure the protection of the rights of data subjects.

[Insert Yes/No]

It is a mandatory requirement for the appointed provider to be registered with the Information Commissioner's Office (ICO). Please confirm that you are registered with the Information Commissioner's Office or will register prior to execution of the contract should your tender be successful.

[Insert Yes / No / Will register]

[Insert ICO registration number if currently registered]

Option B – Low

For medium risk contracts, where there is a moderate-high quantity of low-risk personal data being processed.

GDPR

Please confirm that you have in place, or that you will have in place by the award of the contract, the human and technical resources to perform the contract to ensure compliance with the UK General Data Protection Regulation and to ensure the protection of the rights of data subjects.

[Insert Yes/No]

Please confirm that you have a written data protection and/or information security policy. Please note, the council may request a copy of your policy at preferred bidder stage if your tender is successful.

[Insert Yes/No]

Please confirm that you have secure system(s) for information storage and communication (e.g. Outlook, Dropbox, digital and paper file storage etc) that are encrypted, password protected, and

that processes are in place to restrict access to only those necessary for the delivery of the contract (including process to revoke access to former employees / those that no longer require access)?

[Insert Yes/No]

Please confirm that all employees handling personal data receive given adequate training on data protection and information security?

[Insert Yes/No]

If you have answered 'No' to any of the above, please explain the reasons for this any provide any other relevant information. If you are unable to provide sufficient assurance that personal data will be handled in accordance with UK data protection legislation, your tender may be deemed non-compliant and will not be considered further.

[Insert information]

It is a mandatory requirement for the appointed provider to be registered with the Information Commissioner's Officer (ICO). Please confirm that you are registered with the Information Commissioner's Office or will register prior to execution of the contract should your tender be successful.

[Insert Yes / No / Will register]

[Insert ICO registration number if currently registered]

Option C – Medium

For contracts involving significant levels of personal data and/or some special category data.

GDPR

Please confirm that you have in place, or that you will have in place by the award of the contract, the human and technical resources to perform the contract to ensure compliance with the UK General Data Protection Regulation and to ensure the protection of the rights of data subjects.

[Insert Yes/No]

Please provide details of the technical facilities and measures (including systems and processes) you have in place, or will have in place by contract award, to ensure compliance with UK data protection law and to ensure the protection of the rights of data subjects. Your response should include, but should not be limited to facilities and measures:

- to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services
- to comply with the rights of data subjects in respect of receiving privacy information, and access, rectification, deletion and portability of personal data
- to ensure that any consent-based processing meets standards of active, informed

consent, and that such consents are recorded and auditable

- to ensure legal safeguards are in place to legitimise transfers of personal data outside the UK (if such transfers will take place)
- to maintain records of personal data processing activities
- to regularly test, assess and evaluate the effectiveness of the above measures.

Please use no more than 250 words.

[Insert information]

Option D – High

For high-risk contracts, involving significant levels of personal data and/or some special category data.

Note: ISO and Cyber Essentials accreditations require a material time and financial investment for suppliers. These will be standard for many organisations where processing personal data is a core part of their business (e.g. software providers, educational organisations, and some consultancy firms). However, if the market is composed primarily of micro-businesses or sole traders, it is unlikely that they will have, or be able to obtain, these accreditations.

If you believe this is the case, seek advice from Commercial Services and Information Governance before removing this requirement.

GDPR

It is a mandatory requirement for the appointed provider to hold either a Cyber Essentials Plus certification or be accredited to ISO:27001. Please confirm that you currently hold either Cyber Essentials Plus certification or are accredited to ISO:27001.

[Insert Yes/No]

Please upload evidence of this accreditation/certification.

[Uploaded/Not uploaded]

Please note: the preferred bidder will be required to complete a Supplier Security Assessment form prior to contract award. If you cannot provide a satisfactory response to any questions contained within the Supplier Party Security Assessment form, the council reserves the right not to proceed with the award decision.