DPIA – Data Protection Impact Assessment Policy & Procedure

Document Summary

Staff Lead:	Nicola Addicott
Link Governor:	Fay Reeves
Version Number:	3.0
Document Status:	Approved
Date Last Approved:	December 2025
Date of Next Review:	December 2027
Frequency of Review:	2 Years
Model Policy?	Yes
Statutory Policy?	Yes
On School Website?	Yes

FYI: Version control should be used for all formal documents and managed as:-
▸ **0.1 (1st draft version)** ▸ **0.2 (2nd draft and so on….. 0.3. 0.4 etc)** ▸ **1.0 (Once document has been approved)** ▸ **1.2 (during review/approval of a lifecycle document i.e. policies)** ▸ **2.0 (2nd approved document) and so on.**

Amendment History

Version	Amendment Date	Author	Amendment Summary
V0.0	**110618**	**Mo Jones**	**Formatted from Integra version**
V1.0	**070219**	**Ruth Owen**	**Policy approved at FGB**
V1.1	**010721**	**Ruth Owen**	**Formatted new South Glos Policy**

V1.2	**010721**	**Lucy Gale**	**Update EIA**
V2.0	**301121**	**Ruth Owen**	**Policy approved at FGB**
V2.1	**010425**	**Ruth Owen**	**Updated front sheet ready for review**
V3.0	**200126**	**Ruth Owen**	**Policy approved at FGB**

Equality Impact Assessment (EIA) Part 1: EIA Screening

Policies, Procedures or Practices		Date	11/11/25
EIA CARRIED OUT BY:	Nicola Addicott	EIA APPROVED BY:	Debbie Fisher

Groups that may be affected:

Are there any concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for positive impact
Age (young people, the elderly: issues surrounding protection and welfare, recruitment, training, pay, promotion)	N	N
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication).	N	N
Gender Reassignment (transsexual)	N	N
Marriage and civil partnership	N	N
Pregnancy and maternity	N	N
Racial Groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers	N	N
Religion or belief (practices of worship, religious or cultural observance, including non-belief)	N	N
Gender (male, female)	N	N
Sexual orientation (gay, lesbian, bisexual; actual or perceived)	N	N

Any adverse impacts are explored in a Full Impact Assessment.

Table of Contents

1. Definitions

Initiative - any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity.

Privacy – in its broadest sense the right of an individual to be left alone. It can take two main forms and these can be subject to different types of intrusion:

- **Physical privacy** – the ability of a person to maintain their own physical space or solitude. For example, intrusion can come in the form of unwelcome searches of a person's home or acts of surveillance and the taking of biometric information.
- **Information privacy** – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. For example, intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of information.

Data Protection Impact Assessment (DPIA) – a process which assists the school in identifying, minimising and addressing the privacy risks associated with any new initiative.

Advice sought and consultation – activity to allow people to highlight privacy risks and solutions based on their own areas of expertise. This can include seeking advice from internal stakeholders or formal consultation with external stakeholders including partners or service users

Information Asset – is current information held by the organisation which is categorised from the perspective of its content/ business use rather than necessarily an IT system. It could be a collection of paper or electronic records held by the school that contain customer/ service user, stakeholder, staff or pupil data. The data the asset holds must be personal and/ or sensitive

Personal data - is information about a person which would enable that person's identity to be established. Special category personal data (formerly known as "Sensitive data") is anything which if lost or compromised could affect individuals, organisations or the wider community. Special category personal data is defined by the UK General Data Protection Regulation as including:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- health data (mental or physical);
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning a natural person's sex life or sexual orientation.

2. Background information

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the UK General Data Protection Regulation

With so much information being collected, used and shared in our school, it is important that steps are taken to protect the privacy of each individual and ensure that personal information is handled legally, securely, efficiently and effectively.

Completion of a DPIA will assist us to identify and minimise our privacy risks to comply with our data protection obligations and meet individuals' expectations of privacy.

3. The scope of the policy

The policy covers any initiative considering change, for example a new policy, process, procedure, project, IT system or procurement activity. For the purposes of this policy 'initiative' will cover all of the activity listed above.

The policy provides a process which will enable:

- identification of the need to complete a DPIA through a set of screening questions;
- the collection of sufficient information about an initiative to complete a DPIA;
- privacy risks identified by the DPIA to be documented and considered;

The process should be followed from the start of an initiative to ensure that potential problems are identified at an early stage, when addressing them will be simpler and less costly and the direction of work can be influenced.

Although the policy is aimed at new initiatives information asset owners may wish to use it as a tool to review existing arrangements to identify and address privacy risks as a continuous improvement activity.

4. Duties and responsibilities

The governing body has overall responsibility for the strategic direction and governance of the school, including ensuring that school processes comply with all legal, statutory and good practice guidance requirements.

The Head teacher is responsible to the governing body for ensuring the Information Security

Assurance and Risk Management Plan is implemented and reviewed and its effect monitored. The DPIA is one element of the management of information risk. Information risk needs to be handled in a similar manner to other major risks such as financial, legal and reputational risks.

General staff responsibilities – all school staff must follow the requirements of this and related policies particularly those relating to information governance. Particular care should be taken of the privacy impact of working with contractors and partner organisations.

5. The benefits of a DPIA

The completion of a DPIA is a requirement under UK GDPR and, as such, the ICO may ask an organisation to view a DPIA. It is an effective way to demonstrate to the ICO how personal data processing complies with the UK GDPR.

We can increase pupil, parent and employee confidence in the way we will use their information. An initiative which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

A DPIA will demonstrate transparency and may make it easier to explain to individuals why their information is being used.

It will support our legal obligations under the UK GDPR.

Completing a DPIA in the early stages of an initiative will ensure privacy issues are identified early on and most importantly inappropriate solutions are not implemented that later have to be reversed.

Carrying out a DPIA should benefit the school through better policies and systems being produced and improving relationships with individuals.

6. The DPIA process – key points

The DPIA process is flexible and can be integrated within our existing approach to managing initiatives including those managed through project management arrangements. Appendix B details an overview of the process. The time and resources dedicated to a DPIA should be scaled to fit the nature of the initiative.

A DPIA should begin early in the life of an initiative and should continue to be considered through to implementation.

The DPIA incorporates the following steps:

- identify the need for a DPIA;
- describe the information flows;
- identify the privacy and related risks;
- identify and evaluate the privacy solutions;
- sign off and record the DPIA outcomes;
- integrate the outcomes into the key documentation;
- consult with internal and external stakeholders as needed throughout the process.

7. Guidance for completion of a DPIA

When do I need to complete a DPIA?

You should complete a DPIA at the start of any initiative and use it to maintain awareness and regularly review privacy risks through to completion of work. For procurement activity the DPIA should be completed prior to tender to ensure all relevant privacy risks are considered when preparing specifications.

Who should identify the need for a DPIA and complete it?
It is the responsibility of the lead of an initiative to identify the need for a DPIA and complete it. This may be a process owner, manager of the service area completing the initiative or in the case of formal projects the service lead.

How to identify the need for a DPIA?
The consideration of a number of screening questions will identify the need to complete a DPIA. If any screening question is answered 'yes' a DPIA will need to be completed. The screening questions are detailed in a template attached at appendix C.

How do I complete a DPIA?
The template attached at appendix C will guide staff through the completion of a DPIA.

Why do I need to describe the information flow in a DPIA?
Understanding the information flows involved in an initiative is essential to a proper assessment of privacy risks. Existing processes and resources such as information audits and the Record of Processing Activities (RoPA) can be a useful tool in completing this step of a DPIA. The DPIA template (step two) highlights important information to consider in describing an information flow.

How do I identify a privacy issue and evaluate a solution?
When conducting a DPIA it is necessary to identify any privacy risks and their potential consequences for individuals, compliance and for the school such as fines for noncompliance with legislation or reputational damage leading to loss of trust. The DPIA template (step five) provides a table to record the privacy risks and their consequences. Appendix A provides information about potential privacy risks. The following may also provide useful information:

The ICO's Anonymisation: Managing Data Protection Risk Code of Practice may help to identify privacy risks associated with the use of anonymised personal data.

The ICO's Data Sharing Code of Practice may help to identify privacy risks associated with sharing personal data with other organisations.

The ICO's codes of practice on privacy notices and CCTV, as well as other more specific guidance, will also help to focus DPIAs on those issues.

The DPIA template (step four) provides an optional table to score the level of risk for each privacy risk identified and to evaluate the solution/s identified by measuring the inherent risk score. Any privacy risk with a residual score of 6 or more should be regarded as high risk by the school. It is the responsibility of the school to record relevant risks in the appropriate risk register.

Why do I need to sign off and record the DPIA outcomes?
A key part of the DPIA process is deciding which privacy risks to take forward and recording whether the risks that have been identified are to be tolerated (accepted), treated (reduced), eliminated or transferred. It may be decided that an identified risk is tolerated. However, if there are unacceptable privacy risks which cannot be treated, eliminated or transferred then it will be necessary to reassess the viability of the initiative or a proposal of that initiative. You must record details of the decision maker, who has signed off each risk and the reasons behind their decision.

Who do I need to consult/ seek advice from?
Consultation and seeking advice is an important part of the DPIA process (and can happen at any stage) allowing people to highlight privacy risks and solutions based on their own areas of expertise. Internal activity will be with a range of internal stakeholders for example Governors, Legal, HR, or IT

(this list is not exhaustive, and you need to establish the key internal stakeholders to your initiative). It may take the form of a written communication/ document or verbal discussion taking place in a focus group or project team meeting. External activity provides an opportunity to gain input from people who could be adversely affected by the initiative if privacy risks are not properly considered and addressed. This may take the form of but not limited to electronic consultation or focus groups for service users. The decision to conduct external consultation may be decided as part of the solution to a privacy risk identified.

What documents should be updated?

The DPIA process should be integrated into existing process documents used to plan work required for the initiative. In the case of formal projects this includes the project initiation document (PiD), plan, action/decision, risk/issue log, comms/ consultation plan and the equality impact assessment (if appropriate). The Record of Processing Activities (RoPR) must be updated for any changes made to information assets. Decision reports should include reference to the privacy risks and mitigation identified.

What do I do with completed screening questions and DPIAs?

A copy of the completed screening questions and DPIA should be retained and recorded within the Record of Processing Activity (RoPA) electronic folders for future reference.

How do I report an identified risk?

A key principle of DPIA is that the process is a form of risk management. When carrying out a DPIA you should identify any privacy risks to individuals, compliance risks and any related risks for the school; such as fines for non-compliance with legislation or reputational damage leading to loss of business. (Appendix A refers to possible risks you may wish to consider but remember this is not an exhaustive list and you should consider the risks that relate to your initiative).

The template in Appendix C includes a risk assessment approach which should be followed and if appropriate the risk should be transferred to the risk registers by the Information Asset Owner and to the project risk log. There is the optional table in Step 4 to measure the risk score.

Does a DPIA need to be completed for every initiative?

You must complete the screening questions for every initiative. However you will only need to complete the full DPIA for initiatives that include personal information and for which a screening question has been answered as yes.

8. Monitoring/ review

This policy will be subject to review by the governing body to include effectiveness, compliance and the quality of the assessments completed.

9. Associated documentation

In completing a DPIA you may need to refer to information governance associated policies and guidance.

10. Appendices

Appendix A – Potential privacy risks

Appendix B – Overview of the DPIA process

Appendix C – DPIA template – screening questions and assessment

Appendix A Potential privacy risks

Risks to individuals can be categorised in different ways and it is important that all types of risk are considered – these range from risks to physical safety of individuals, material impacts (such as financial loss) or moral (for example, distress caused). Possible risks include:

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 organisations 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 UK GDPR 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 school.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of confidence.
- Data losses which damage individuals could lead to claims for compensation.

Compliance risks

- Non-compliance with the UK GDPR
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR)
- Non-compliance with school specific legislation or standards
- Non-compliance with human rights legislation

Appendix B Overview of the DPIA process

Step 1: Identifying the need for a DPIA
The need for a DPIA can be identified using the screening questions included in the DPIA template – see Appendix C.

Step 2: Describing the processing Where the screening questions identify the need for full DPIA see Appendix C.
Describe the information flows of the initiative. Explain what categories of personal data will be collected and how it is collected, how it is used, stored and deleted, what it is used for, who it is obtained from and disclosed to, who will have access, and any other necessary information. For existing data establish that original consent and privacy notices cover the work being planned/undertaken.

Step 3: Consultation with stakeholders
Consider when and how to seek individuals views (or justify why it's not appropriate to do so). Who else should you involve within school or do you need to consult with third party experts?

Step 4: Compliance, Necessity and Proportionality
Explain the legal basis for processing personal, special category or criminal data. Is there is another way to achieve the same outcome? What information will be given to individuals about processing their data? Data collected must be relevant to this initiative and no more than required to achieve the purpose, data must only be used for the purpose that it is collected. Explain how it will be kept up to date and not stored for longer than necessary.

Step 5: Identify, Assess and reduce Risks

- some will be risks to individuals – for example damage caused by inaccurate data or security breach, or upset caused by unnecessary intrusion on privacy.
- some risks will be to the organisation – for example damage to reputation, or the financial costs of a data breach.
- legal compliance risks include the UK GDPR, PECR, and the Human Rights Act.

Explain how you could address each risk. Some might be eliminated altogether. Other risks might be reduced. Most initiatives will require acceptance of some level of risk, and will have some impact on privacy.

Step 6: Authorisation / Sign off and recording the DPIA outcomes
Privacy risks must be signed off at an appropriate level as part of the decision making process.

A DPIA report should summarise the process, and the steps taken to reduce the risks to privacy. It should also record the decisions taken to eliminate, mitigate, or accept the identified risks.

Publishing a DPIA report will improve transparency and accountability and lets individuals learn more about how your project affects them.
The DPIA findings and actions should be integrated back into key documentation It might be necessary to return to the DPIA at various stages of the initiative's development and implementation. Large initiatives are more likely to benefit from a formal review process.

A DPIA might generate actions which will continue after the assessment has been finished and these must continue to be monitored. Record what you can learn from the DPIA for future initiatives on the Record of Processing Activity spreadsheet (RoPA) which is held on the shared Admin drive.

Appendix C DPIA template for screening questions and completing an assessment

Data Protection Impact Assessment
Part 1 – Guidance & Screening Questions

How to use this DPIA template

Our DPIA template is split into two parts:

Part 1: DPIA Guidance and Screening Questions.
This section will help you to identify whether the processing of personal data is (a) necessary and (b) likely to result in a high risk to individuals requiring the completion of a full DPIA. Use the screening questionnaire on the following pages to record the outcome of your DPIA screening exercise.

Part 2: Full DPIA.
Where one or more of the mandatory screening questions are answered YES, a full DPIA will be required. (See Part 2 of this template).

If you are unsure whether you need to complete a full DPIA, please return your *completed* screening questionnaire to i-west@bathnes.gov.uk We will review it for you and advise whether a full DPIA is needed.

More information on how to complete a DPIA more generally can be found in Appendix 1.

What is a Data Protection Impact Assessment?

A Data Protection Impact Assessment (DPIA) is a risk assessment to help you to identify and minimise data protection risks associated with processing personal data.

Under the UK GDPR it is a legal requirement to complete a DPIA for any processing (use) of personal data that is likely to result in a *high risk* to individuals. This includes changes to existing processes, as well as new projects. You can use this screening questionnaire to determine whether your project/system/processing is high risk and requires a DPIA. The DPIA should be undertaken before processing commences.

It is also best practice to complete a DPIA for any major projects that require you to process personal data, such as the adoption of new information systems and services. As well as meeting the legal requirement, completing a DPIA could help avoid unnecessary costs, help protect your reputation, and provide assurance to stakeholders, such as your Audit & Risk Committee, about the safety of processing.

Who should complete the DPIA?

The DPIA should be coordinated by the project lead or somebody who has a good understanding of what the processing will involve. Completion of the DPIA is likely to need the involvement of several stakeholders e.g. IT, HR, system provider, and end users, and shouldn't rest with one person solely.

It is a legal requirement to consult your Data Protection Officer (DPO) regarding the completion of a DPIA. The DPO's role is to advise on and monitor the DPIA. It is not the DPO's responsibility to complete the DPIA as they will not have enough knowledge of the project or processing involved.

Organisation	
Project name	
Project manager	
Date	Click or tap to enter a date.

1. Aim & Purpose of the project / processing
What are you hoping to achieve from this project / change? Why is it necessary? Is it for compliance with a legal obligation or statutory guidance?
The aim of the project is to: enter the aim of this processing. This is: select whether this is new processing or changes to existing processing Without this project / change: explain what the impact would be if this doesn't happen. The project / processing is necessary because: explain why the processing is necessary. The legislation / statutory guidance this project supports (if applicable) is: enter legal/regulatory requirements.

2. Higher Risk Factors	**Yes**	**No**
1. Will the project involve **large scale processing** of personal data?	☐	☐
2. Will the project involve **profiling** or **monitoring or automatic decision making**?	☐	☐
3. Does the project involve **special category* or criminal offence data** or the use of the personal data of **vulnerable individuals (including children)**? **special category data includes: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data, health information, sex life or sexual orientation.*	☐	☐
If you've answered YES to any of the questions above, it is highly recommended that you conduct a DPIA regardless of the mandatory screening questions below. If you decide not to complete a DPIA, then you should retain this form along with a record of your decisions. Please contact the DPO for advice.		

3. Mandatory Risk Factors for a full DPIA This project does / will…	Yes	No
1. Use systematic and extensive profiling or automated decision-making to make significant decisions about people.	☐	☐
2. Process special category or criminal offence data on a large scale.	☐	☐
3. Systematically monitor a publicly accessible place on a large scale (e.g. CCTV).	☐	☐
4. Use innovative technologies or the novel application of existing technologies (including AI) (e.g. innovative systems, programs, websites, databases etc.)	☐	☐
5. Use profiling or special category data to make decisions on someone's access to a service, opportunity, or benefit.	☐	☐
6. Profile individuals' personal data on a large scale.	☐	☐
7. Use biometric data, such as fingerprints and facial features (e.g. for cashless catering, or access controls).	☐	☐
8. Use genetic data, such as an individual's gene sequence.	☐	☐
9. Combine, compare or match datasets from multiple sources.	☐	☐
10. Use personal data that has not been obtained directly from the data subject without providing a privacy notice to the individual.	☐	☐
11. Use personal data in a way that involves tracking individuals' online or offline location or behavior.	☐	☐
12. Process children's or other vulnerable individuals' personal data for marketing purposes, profiling or automated decision-making. Or offering online services directly to children.	☐	☐
13. Risks physical harm in the event of a security breach.	☐	☐

If you answered 'YES' to any of the questions in section 3 above, then you must complete a full DPIA (please use **Part 2** of this template).

Please note that it is best practice to complete a DPIA (risk assessment) whenever you undertake a major project involving the use of personal data.

DPO Review

DPO Name	Click or tap here to enter One West representative name.
Date of DPO Review	Click or tap to enter a date.
DPO Advice	Click to select.

Appendix 1 – Further information

Crucially, a DPIA needs to:

- Describe the nature, scope, context and purposes of the processing
- Assess necessity, proportionality and compliance of processing.
- Identify and assess risks to individuals.
- Describe any additional measures to mitigate those risks.

A DPIA should be done early in the life of a project. Certainly, before you start the processing, but ideally during the planning and development phases of a project. Importantly, assessing risk this way is a cyclical activity – see the diagram below.

Figure 1 - DPIA Cycle

A crucial part of the process involves consulting with your DPO, One West. One West is there to help and ultimately One West will have to sign-off the DPIA.

Note, if you identify a high risk that you cannot mitigate, you may need to consult the ICO. Again, One West will advise you if that is the case and help prepare a question for the ICO.

Who is responsible for carrying out a DPIA?

The data controller is ultimately responsible for completing a DPIA although they can allocate the task to someone who would be responsible day-to-day for that processing. For example, the Head of HR or the Business Manager, who probably know most about the organisation's HR system, might be given the job.

Importantly, the assessor may also need to work with internal experts, such as the Head of IT, as well as other processors (contractors) and certainly the supplier / vendor to get an accurate view of risk/s.

Again, the assessor can consult with One West while completing the DPIA. For new processes / services the project lead should contact the DPO, as early as possible.

Note it is not the DPO's responsibility to complete the DPIA. They do not have complete knowledge of the data processing activity. Nonetheless, they may have encountered similar risk while working with other trusts / schools.

This dialogue with the DPO should be recorded as part of the process.

Data Protection Impact Assessment

Part 2 – DPIA Remplate (Full DPIA)

Process

1. Complete Part 1 DPIA Screening Questionnaire.
2. If the Screening Questionnaire identifies the necessity for a full DPIA, complete Part 2 'Full DPIA Template' (see instructions below):
    a. Complete steps 1-5
    b. Send your draft DPIA to i-west@bathnes.gov.uk
    c. Complete step 6 and retain the final DPIA for reference, along with Part 1 Screening Questionnaire.
    d. Review your DPIA annually (or when risk identified).

Instructions for completing Part 2 'Full DPIA Template'

The following DPIA template includes a series of steps to follow. At each step there are several questions relating to the processing that you will need to answer.

In some cases, we have provided either a drop-down list or a series of likely answers plus the facility to write your own answers should none in the list fit with your circumstances. In some cases, we have provided a simple text field for you to write your answer.

Step 5 'Identify, Assess and Reduce Risks' is key to your organisation's understanding and mitigating risks. ***We have included examples to get you started (Appendix 1) – please do not just copy and paste these risks into the table (unless they apply) They are intended to help you think about the specific risks relating to your own proposed use of personal data.***

Please note that the risk assessment and solution assessment fields are in drop-down lists for you to pick from.

If you have any questions about filling out this form, please consult your DPO:

i-west@bathnes.gov.uk

Step 1: Identify the need for a DPIA

1.1 Project Details		
Organisation		Enter your organisation name
Project name		Enter project name
Project manager / lead		Enter details of Project Manager or Lead
Version no.	**Version date**	**Summary of key changes**
1		First draft

1.2 The need for a DPIA

You do not need to complete this section as this will be detailed in Part 1 of the Screening Questionnaire.

Step 2: Describe the processing

2.1 Nature of the processing

2.1.a How will/do you collect, use, store and delete the personal data?

How we collect the data	
How we use the data	
How we store the data	
How we delete the data	

2.1.b What is the source of the data?

2.1.c Who will you be sharing the data with? (E.g. Local Authority, other public bodies etc.)

2.1.d What type of processing have you identified as high risk?

See Part 1 Screening Questionnaire

2.2 Scope of the processing

2.2.a What categories of personal data will be processed? Does it include special category or criminal offence data?

Identifiers e.g. *names, username, photo, video footage, recordings, vehicle registration.*	☐
Contact details e.g. *email address, home address, telephone number.*	☐
Physical characteristics e.g. *height, age, DoB, hair colour, skin tone, tattoos, piercings.*	☐
Family e.g. *family structure, siblings, offspring, marriages, divorces, relationships.*	☐
Behavioural e.g. *browsing behaviour, call logs, links clicked, demeanour, attitude.*	☐
Professional e.g. *job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary*	☐
Financial e.g. *credit card number, bank account.*	☐
Device e.g. *IP/Mac address, browser fingerprint, serial number, device license plate*	☐
Racial or ethnic origin	☐
Political opinions	☐
Religious or philosophical beliefs	☐
Trade Union membership	☐
Genetic & biometric Data	☐
Health information (mental or physical health)	☐
Sex life or sexual orientation	☐
Details of criminal offences / convictions	☐
Other: …click to add details.	

2.2.b How much personal data will you be collecting and using? How often? How many individuals are affected by the processing?

For example (i) How many officers/staff/pupils/residents? (ii) What specific data fields will you be processing – e.g. name, address, mobile no, DoB, ethnicity (iii) How frequently will you be collecting it?

2.2.c How long will you keep the data? How will you ensure it is deleted in line with your retention policy?

2.3 Context of the processing
2.3.a What is the nature of your relationship with the individuals?
2.3.b How much control will individuals have over the processing of their data?
2.3.c Would individuals expect you to use their data in this way? Are they aware of it?
2.3.d Does the processing include children or other vulnerable individuals?
2.3.e Are there prior concerns over this type of processing or security flaws?
2.3.f Is the processing novel in any way? What is the current state of technology in this area?
2.3.g Are there any current issues of public concern that you should factor in?
2.3.h Do you have any accreditations relevant to privacy / security? E.g. ISO 27001, Cyber Essentials
NB: If the provider has security/privacy accreditations then please detail these in 4.2.g (p10)

2.4 Purposes of the processing
2.4.a What do you want to achieve?
2.4.b What is the intended effect on individuals?
2.4.c What are the benefits of the processing – for your organisation and more broadly?

Step 3: Consultation

3.1 Consultation with stakeholders
3.1.a When and how will you seek individuals' views? (or justify why it's not appropriate to do so).
3.1.b Who else do you need to involve (or have involved) within your organisation and how will you engage with them?
3.1.c Do you need to ask any third party / data processors to assist?
3.1.d Do you plan to consult information security experts, or any other experts?

Step 4: Compliance, Necessity and Proportionality

4.1 Lawfulness

Use drop down lists. The DPO can complete this section if you are unsure

4.1.a What is your lawful basis (or bases) for processing?

The legal basis for processing of personal data (Article 6) is: …choose from drop-down list.

If applicable: The specific legislation relating to this processing is …provide details of legislation or regulation relating to your organisation's legal obligation or public interest duties.

4.1.b What is your condition for processing special category data? (select N/A if you are not processing special category data)

The special category data condition for processing (Article 9) is: …choose from drop-down list.

If applicable The associated condition under the Data Protection Act 2018 Schedule 1 is: Enter DPA 2018 Schedule 1 condition.

4.1.c What is your Article 10 basis for processing criminal offences/convictions? (select N/A if you are not processing criminal offence data)

The Article 10 condition for processing criminal offence data is: …choose from drop-down list.

If applicable The associated condition under the Data Protection Act 2018 Schedule 1 is: Enter DPA 2018 Schedule 1 condition.

4.2 Fairness, necessity and proportionality
4.2.a Is there another way to achieve the same outcome?
4.2.b What information will you give to individuals about the processing of their data?
4.2.c How will you prevent function-creep? i.e. make sure that the personal data being used for this project/process isn't used for something else.
4.2.d How will you ensure that your use of the personal data is adequate, relevant and no more than necessary to achieve your purpose? How will you ensure data minimisation?
4.2.e How will you ensure data quality and accuracy? How will it be kept up to date?
4.2.f How will you ensure that the data isn't stored in an identifiable format for longer than necessary?

4.2.g How will you ensure that personal data is protected against unauthorised / unlawful use, accidental loss, damage or destruction?
What technical and organisational security measures will be put in place to protect the data?
How will you make staff aware of any security measures or procedures they need to follow?
4.2.h How will you ensure that individuals can exercise their data protection rights?
4.2.i How will you ensure that data processors comply with the requirements of any contracts / data processing agreements?
4.2.j How will you safeguard any international transfers? (contact DPO if unsure)
Where will personal data be hosted? Include routes of transfer if data leaves the UK (for example, while most Microsoft cloud services are based in Europe, the data sometimes goes via America)
If the personal data leaves the UK, explain which of the formal / recognised adequacy measures are in place (DPO can advise):

Step 5: Identify, Assess and Reduce Risks

Please complete the Risk Assessment below with specific risks relating to the processing and how you will mitigate the risks.
Consider the practical / day to day risks that apply to your project/processing. E.g. Could personal data be downloaded to a non-secure device? Could sensitive data be inadvertently displayed on a classroom whiteboard? Could data be saved to a memory stick which could be lost?

*You will find examples of potential risks and solutions in the table shown in **Appendix 1**.*

You can add additional rows ('right click, insert, insert row') or delete rows ('right click, delete row') as needed.

Risk	**Select from dropdown list**			**Solutions**	**Select from dropdown list**		
	Likelihood of harm Remote/ Possible/ Probable	**Severity of harm** Minimal/ Significant/ Severe	**Overall risk level** Low, medium or high		**Effect on risk** Eliminated/ Reduced/ Accepted	**Residual risk** Low/ Medium/ High	**Solution approved** Yes/no
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.

Risk	Select from dropdown list			Solutions	Select from dropdown list		
	Likelihood of harm Remote/ Possible/ Probable	**Severity of harm** Minimal/ Significant/ Severe	**Overall risk level** Low, medium or high		**Effect on risk** Eliminated/ Reduced/ Accepted	**Residual risk** Low/ Medium/ High	**Solution approved** Yes/no
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.
What is the risk?	Choose an item.	Choose an item.	Choose an item.	What is the solution?	Choose an item.	Choose an item.	Choose an item.

Step 6: Authorisation / Sign-off

DPIA authorisation		
Measures approved by:	Enter name	Enter a date.
Residual risk approved by *If accepting any residual high risk, consult the ICO before going ahead*	Enter name	Enter a date.
Date of consultation with DPO	Enter a date.	
Summary of DPO advice		
DPO advice accepted or over-ruled by Project Manager / Sponsor	DPO advice is: …choose from drop-down list.	
Rationale for over-ruling the DPO's advice (if applicable)		
Date and name of person referring DPIA to ICO (if applicable)	Enter name	Enter a date.
Summary of ICO advice (if applicable)		
Date of updating Record of Processing Activity	Enter a date.	
Date of next review	Enter a date.	

Appendix 1 - Example Risks and Solutions

The table below includes examples of potential risks that might arise and some suggested solutions. This list is not exhaustive, and you should work with key stakeholders to identify specific risks.

Example risks	***Example solutions***
Loss or theft of personal data due to external attack by third party e.g. cyber attack	*IT Lead/provider will advise on appropriate security including firewalls and password controls.*
Unauthorised access of personal data due to loss of device (laptop, mobile phone etc).	*Multi factor authentication is in place. All devices are encrypted. Password requirements are in line with NCSC advice. Device can be remotely wiped.*
Unauthorised use or sharing of personal data by staff (e.g. downloading data onto unsecure memory stick, copying data out of the system and saving it elsewhere).	*Access rights will be tightly controlled and reviewed regularly by IT. Staff receive annual data protection training and are subject to the Acceptable Use Policy. Memory sticks are not permitted.*
Data is not backed up and cannot be accurately restored leading to loss of data (data breach).	*Data is regularly backed up to a separate server.*
Data is inaccurate or out of date leading to unsafe decisions being made (e.g. personal data sent to wrong address).	*Data is drawn from the main MIS system which is maintained by the Business Support Manager and updated regularly.*
Data which is required to be deleted cannot be securely deleted in line with the organisation's retention policies.	*Essential criteria for selecting the new system provider will include technical solution for permanent deletion.*
Processing of personal data is not fair or lawful. Data subjects are not expecting their data to be processed in this way leading to complaints to the ICO.	*DPO has advised on lawful basis. Communications will be sent to data subjects and Privacy Notice has been updated.*
Data subjects not able to exercise their rights (e.g. data cannot be extracted for a Subject Access Request or transferred in a machine-readable format).	*Essential criteria for selecting the new system provider will include technical solution for data extraction in accordance with requirements of UK GDPR.*
Data contained within the system is not limited to that which is necessary and is excessive.	*Data is drawn from the main MIS system which is maintained by the Business Support Manager and updated regularly. System users are trained on data entry requirements.*

Annex 1 – Linking the DPIA to the UK General Data Protection Principles

This annex will help you identify where there is a risk that the initiative will fail to comply with the UK General Data Protection Regulation or other relevant legislation. The principles listed are those set out in Article 5 of the UK General Data Protection Regulation with italic notes explaining the information you need to consider.

NB - The wording refers to projects using a broad definition and for the purposes of conducting a DPIA should be applied to any initiative.

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

Have you identified the purpose of the project?

How will individuals be told about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

Are your actions a proportionate response to the need?

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

Does your project plan cover all of the purposes for processing personal data?

Have potential new purposes been identified as the scope of the project expands?

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

Is the information you are using of good enough quality for the purposes it is used for?

Which personal data could you not use, without compromising the needs of the project?

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

What retention periods are suitable for the personal data you will be processing?

Are you procuring software which will allow you to delete information in line with your retention periods?

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

In addition to the Principles in Article 5, Chapter V covers data being transferred to another country outside the UK

Will the project require you to transfer data outside of the UK?