



Information Security Document

**Electronic Kitchen Management
System (EKMS) Privacy Impact
Assessment**

Version 1.3

Version History			
Version	Date	Detail	Author
1.0	15/06/2017	First Draft for consideration by working group	
1.1	29/06/2017	Revised version for consideration by working group	
1.2	30/06/2017	Post working group version	
1.3	11/07/2017	Amended by Information Governance Group and Procurement Officer's Group.	
This document has been prepared using the following ISO27001:2013 standard controls as reference:			
ISO Control		Description	
A.18.1.1		Identification of applicable legislation and contractual requirements	
A.18.1.3		Protection of records	
A.18.1.4		Privacy and Protection of personally identifiable information	

CONTENTS

Contents	Page
Introduction	4
What is a Privacy Impact Assessment (PIA)?	4
When will a PIA be appropriate?	4-5
What is meant by Privacy?	5
Informational Privacy Risk	5-6
The Benefits of a PIA	6
Projects which might require a PIA	7
PIA Procedure	7
Monitoring	7

1. Introduction

A privacy impact assessment (PIA) is a tool which can help the Council identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy.

An effective PIA will allow the Council to identify and fix problems at an early project stage, reducing the associated costs and damage to reputation which might otherwise occur.

This policy explains the principles which form the basis for a PIA.

The main body of the policy sets out the basic steps which the Council should carry out during the assessment process.

Templates are at Annex A and B

2. What is a Privacy Impact Assessment (PIA)?

A PIA is a process which helps an organisation to identify and reduce the privacy risks of any project.

The PIA process is not new to the Council. Privacy implications are already considered as part of the project planning process. However, the aim of this procedure is to ensure that this is done on a systematic and consistent basis.

To be effective a PIA should be used throughout the development and implementation of a project, using existing project management processes.

A PIA will enable the Council to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.

3. When will a PIA be appropriate?

PIAs will be applied to new projects, because this allows greater scope for influencing how the project will be implemented.

A PIA can also be useful when planning changes to an existing system.

A PIA can also be used to review an existing system, but the organisation needs to ensure that there is a realistic opportunity for the process to implement necessary changes to the system. However, the Council does not propose to review existing systems at this point in time.

The main purpose of the PIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met.

Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice.

This analysis can be tested by consulting with people who will be working on, or affected by, the project.

Conducting a PIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the privacy risks arising.

A PIA should be undertaken before a project is underway.

4. What is meant by Privacy?

Privacy, in its broadest sense, is about 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. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
- Informational privacy – the ability of a person to control, edit, manage and delete information about them and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

5. Informational Privacy

This policy is concerned primarily with minimising the risk of informational privacy - the risk of harm through use or misuse of personal information.

Some of the ways this risk can arise is through personal information being:

- inaccurate, insufficient or out of date;
- excessive or irrelevant;
- kept for too long;
- disclosed to someone where the person who it is about does not want them to have it;
 - used in ways that are unacceptable to or unexpected by the person it is about;
- or
- not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal relationships and social standing arising from disclosure of confidential or sensitive information.

Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised. There is also harm which goes beyond the immediate impact on individuals. The harm arising from use of personal information may be imperceptible or inconsequential to individuals, but cumulative and substantial in its impact on society. It might for example contribute to a loss of personal autonomy or dignity or exacerbate fears of excessive surveillance.

The outcome of a PIA should be a minimisation of privacy risk.

6. The Benefits of a PIA

The Information Commissioner's Office (ICO) promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits.

Conducting a PIA is not a legal requirement of the DPA, but carrying out an effective PIA should benefit the people affected by a project and also the organisation carrying out the project. It is also a requirement of the Information Governance Toolkit Assessment to show that PIAs are undertaken.

Whilst a PIA is not a legal requirement, the ICO may often ask an organisation whether they have carried out a PIA. It is often the most effective way to demonstrate to the ICO how personal data processing complies with the DPA.

Conducting and publicising a PIA will help the Council to build trust with the people using their services.

The actions taken during and after the PIA process can improve an organisation's understanding of their customers.

There can be financial benefits to conducting a PIA. Identifying a problem early will generally require a simpler and less costly solution. A PIA can also reduce the ongoing costs of a project by minimising the amount of information being collected or used where this is possible, and devising more straightforward processes for staff.

More generally, consistent use of PIAs will increase the awareness of privacy and data protection issues within an organisation and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a PIA would be appropriate

- A new IT system for storing and accessing personal data.

- A data sharing initiative where two or more organisations seek to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new database which consolidates information held by separate parts of an organisation.
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring.
- Cloud hosted applications
- The collection of new data on an existing system

A PIA should be used on specific projects and to be effective it should be applied at a time when it is possible to have an impact on the project. This means that PIAs are more likely to be of use when applied to new projects or revisions of existing projects. Procurement practices and procedures are key to the success of this procedure and will be adapted accordingly.

The Council must identify the need for a PIA at an early stage and build this into project management or other business processes.

The Client Department (Commissioner) will be responsible for carrying out the PIA.

7. PIA Procedure

The format for an initial PIA is at **Annex A**.

This review form is based on the eight Data Protection Principles described in Schedule 1 of the Data Protection Act.

In the event that a full PIA is deemed appropriate the format for this is at **Annex B**

The links between the PIA and DPA are set out in **Annex C**

8. Monitoring

The completed PIA should be submitted to the Information Governance Group (IGG) for monitoring purposes.

The IGG will also monitor implementation of actions identified in PIA's

This procedure will be reviewed in June 2018.

Annex A

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?

Will the project compel individuals to provide information about themselves?

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.

Will the project require you to contact individuals in ways that they may find intrusive?

Annex B

Privacy impact assessment template

This template is an example of how you can record the PIA process and results. You can start to fill in details from the beginning of the project, after the screening questions have identified the need for a PIA. The template follows the process that is used in this code of practice. You can adapt the process and this template to produce something that allows your organisation to conduct effective PIAs integrated with your project management processes.

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

As a traded service to schools the Catering Service provides to Schools and Academies.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Currently there is no immediate method of electronic communication between back office and kitchen staff. Not only is there a lack of hardware to support this (none in Primary School kitchens) but there is no process in place to routinely connect DCC equipment to school networks. Therefore, information to kitchens and return information, for example, letters, mandatory data returns, training updates and Health and Safety updates are delivered in hard copy using the internal mail system via the Derbyshire Business Centre. The process can be drawn-out with an approximate two week turnaround. Estimated cost is £20k annually.

The only method available for urgent information to be communicated is via telephone calls from Caterers to their individual school patches. With only 7 Caterers covering over 250 cooking kitchens this process is time consuming, unreliable and inefficient.

Meals provided to Primary Schools are charged to schools on a four weekly basis. Currently the figures are based on the completion of Meal Reconciliation (MR1) paper forms which are submitted by the schools to the service. The form provides written confirmation of meals prepared/served per day. The figures are given to Caterers on a weekly basis either by telephone or text message and collated on Excel spreadsheets. The input process is time consuming and is usually in arrears by one month. The chasing of late returns and the correction of written errors on the form can be time consuming. This heavily impacts on the financial statistics required by Accountancy to facilitate forecasts, projections and costs for the forthcoming financial periods.

The objectives of the system to the Council and stakeholders:

- To provide a web based externally hosted Kitchen Management Solution by June 2018.
- To provide fully supported compatible hardware by June 2018.
- To purchase training materials for the chosen solution by June 2018.

The benefits of the system to the Council and stakeholders:

- Administration will be streamlined – with the reduction of printing and postage costs
- Increased management effectiveness as processes will be streamlined
- Improved legislative compliance at kitchen level
- Purchase orders raised via the system will eliminate the costs of printing of PLOFs (paper based order forms) and also provide an appropriate audit trail
- Identification of individual school costs on demand, identifying spending trends and possible fraudulent action
- Improvement of management effectiveness allowing managers to identify low meal uptake with schools and high food costs
- Improved communication with kitchens to maximise efficiency and working relationships.

It has been identified that a PIA is required under Corporate Policy as personal data will be held within the new system and new processes will be introduced which involve entering and using individual staff and pupil data.

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

The collection of sensitive information within Derbyshire Catering Services (DCS) is minimal and consists primarily of staff records relating to training, accident reporting, absence, one to ones and working hours. In addition to which, records for pupils requiring medical diets will be stored.

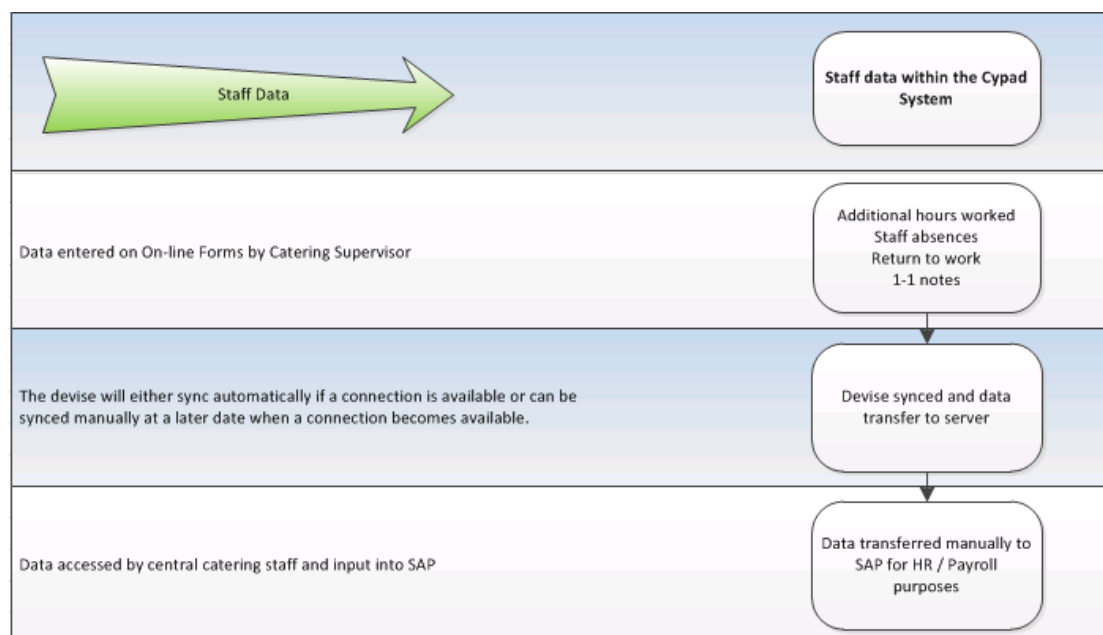
Data held within the electronic kitchen manager will be primarily inputted by the Catering Supervisor based within the kitchen. This information will be uploaded on a “to be determined” frequency from individual kitchens using standard template forms requiring population only.

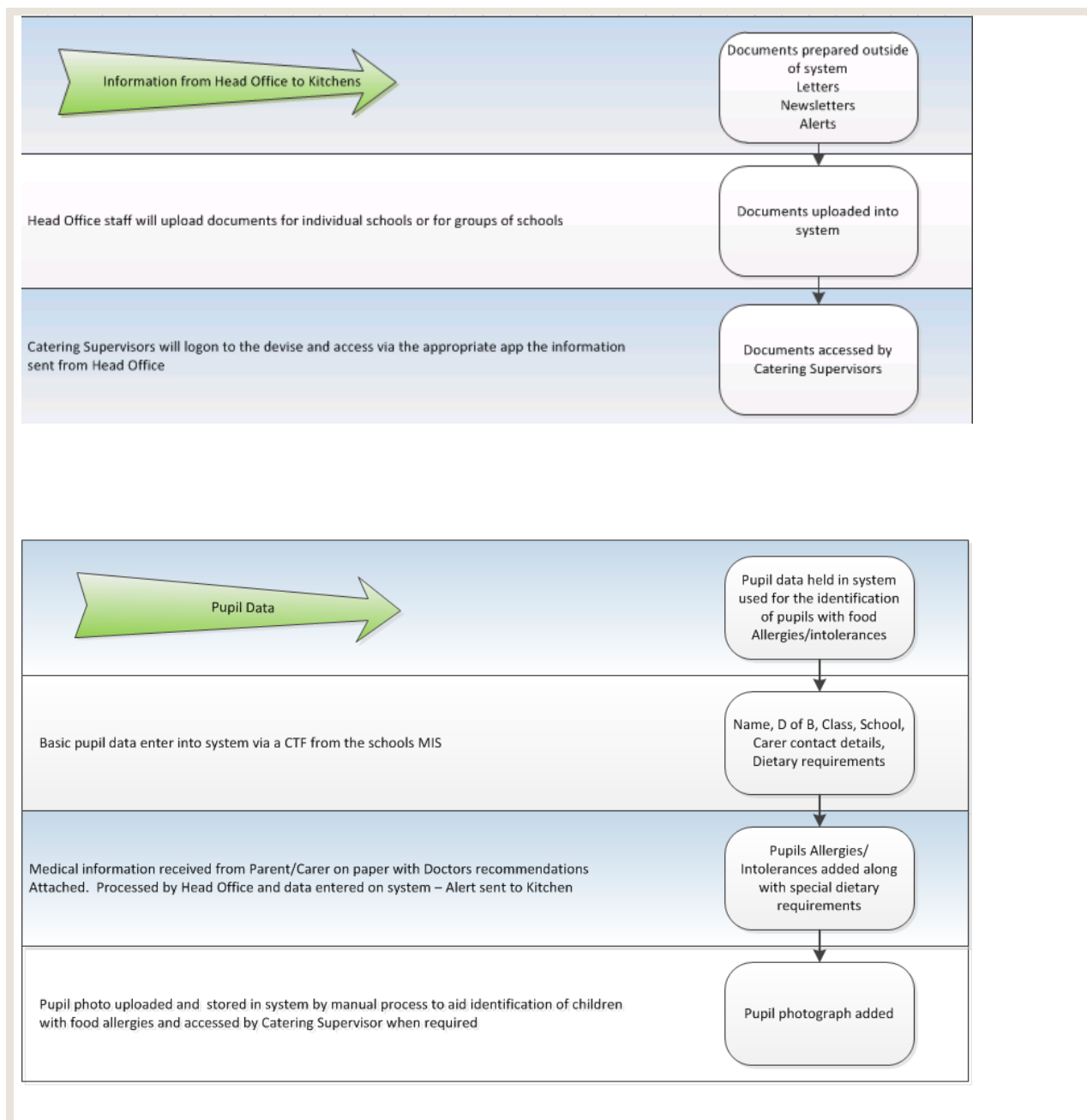
Information stored will be transferred to central departments for example Shared Services using either email or customised reports as determined by DCS and influenced by the outcome of the Audit QA report.

It will be the responsibility of the senior management team within DCS to identify employees who should have the appropriate role based access to view the data and restrict access to unauthorised users.

Authorised users will review the information on an annual basis as a minimum removing pupil leavers information as appropriate. Ad hoc pupil leavers information will be data cleansed when identified. Maintenance of the information will be the responsibility of the Catering Supervisor.

Maintenance of staff Information will be managed in line with DCC policy.





Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

During the whole process of procuring a kitchen manager system, reviews have taken place with stakeholders, staff, schools and any interested parties within the Authority.

Groups	Method of Communication
Schools	Using Servies4 Schools communication portal
Cypad	Direct via email/phone
Governors	Via Governor newsletter – once approval granted
Suppliers	Direct via email and one to one meeting
Academies	Using Services 4 Schools communication portal
Parents	Via School newsletters and school, My School Lunch and Derbyshire.gov.uk websites

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

Annex C can be used to help you identify the DPA related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Non-compliance with data protection act	Individuals privacy is compromised	Regulatory action	Financial and reputational damage
Data is accessed by unauthorised persons	Risk to individual as a contravention of their rights	Regulatory action	Financial and reputational damage
Data maintenance to ensure information held is relevant, up to date and accurate	Breach of data protection act	Regulatory action	Financial and reputational damage
Risk of personal information being accessed without the consent of the individual/parent/carers/employee	Individuals data is shared beyond what is expected	All organisations to comply with the data sharing arrangements	Financial and reputational damage
Risk of additional records being added without the knowledge of employees	Individuals data is shared beyond what is expected	All organisations to comply with the data sharing arrangements	Reputational damage
Inadequate disclosure controls and risk information being shared inappropriately	Personal information shared	Breach of data protection	Data breached

Data is used for unauthorised purposes

Personal information shared

Breach of data protection

Financial and reputational damage

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution(s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
As detailed in step three	Training All staff to receive the appropriate training on data protection procedures (Safe Haven Protocols)	Reduced	Yes
	Guidance Circulate to all staff data Derbyshire County Council protection protocols.	Reduced	Yes
	Seek guidance from Data Protection Officer to ensure compliance in all aspects of information stored	Reduced	Yes
	Validation Determine validation checks on the data stored meets data protection requirements and information retention responsibilities	Reduced	Yes

	Auditing Review accuracy of data stored. Ensure correct processes are followed in accordance with DCC policy	Reduced	Yes
	Monitoring Set periodic monitoring targets to check validity of data, employee access levels and data cleansing	Reduced	Yes

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by
As identified in step three	Departmental risk register completed and approved by Jane Morgan	Kathryn Boulton Service Director Tim Blowers Head of Catering Services

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action
Review training plan prior to ensure adequate training provided Liaise with [REDACTED] for Data Protection to ensure the appropriate procedures are in place	Post implementation	[REDACTED]

Contact point for future privacy concerns

A black rectangular redaction box covers the contact information provided below the heading.

Annex C

Principle 1 - Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless: a) at least one of the conditions in Schedule 2 is met, and b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.	
Have you identified the purpose of the project?	Yes
How will you tell individuals about the use of their personal data?	Organised training events
Do you need to amend your privacy notices?	Yes Staff /Pupil –
Have you established which conditions for processing apply?	Yes
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?	Consent will be required for pupil data to be stored and used – this will be covered on the Schools Privacy Notice (Will require amendments)
If your organisation is subject to the Human Rights Act, you also need to consider:	
Will your actions interfere with the right to privacy under Article 8?	Yes
Have you identified the social need and aims of the project?	Yes
Are your actions a proportionate response to the social need?	Yes

Principle 2 - Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	
Does your project plan cover all of the purposes for processing personal data?	Yes
Have you identified potential new purposes as the scope of the project expands?	Yes

Principle 3 - Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	
Is the quality of the information good enough for the purposes it is used?	Yes

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

Principle 4 - Personal data shall be accurate and, where necessary, kept up to date.	
If you are procuring new software does it allow you to amend data when necessary?	Yes
How are you ensuring that personal data obtained from individuals or other organisations is accurate?	

Principle 5 - Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.	
What retention periods are suitable for the personal data you will be processing?	Five – Seven years
Are you procuring software that will allow you to delete information in line with your retention periods?	Yes

Principle 6 - Personal data shall be processed in accordance with the rights of data subjects under this Act.	
Will the systems you are putting in place allow you to respond to subject access requests more easily?	Yes
If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?	N/A

Principle 7 - Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	
Do any new systems provide protection against the security risks you have identified?	Yes
What training and instructions are necessary to ensure that staff know how to operate a new system securely?	New equipment training programme Data Governance / Security will be part of the training

Principle 8 - Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?	No
If you will be making transfers, how will you ensure that the data is adequately protected?	No personal data will be transferred from the system.