UCISA TOOLKIT

Privacy Impact Assessment

ucisa
Universities and Colleges
Information Systems Association

Universities and Colleges
Information Systems Association

Contents

1 Introduction

The volume of personal information processed today dwarfs that processed five years ago, and will be dwarfed by the volume that will be processed in five years' time. The rise of social media, smart phones, the Internet of Things, wearable technology and big data means that the levels of scrutiny we are all subject to is unprecedented. Typically, people tend not to worry too much about what information is gathered, who gathers it, what it is used for and who it is shared with. That is, until a data leak occurs, or an individual suffers identity theft or payment card fraud, at which point questions tend to be asked about how organisations capture, use and safeguard personal data.

Principle Seven of the *Data Protection Act 1998* [1] (DPA) and Article 32 of the *General Data Protection Regulation*[2] (GDPR) require that appropriate technical and organisational measures are taken to safeguard personal data. This places a requirement on organisations to have in place adequate information security measures, and a wealth of information is available on this topic, including the UCISA Information Security Management Toolkit[3].

However, the responsible use of personal data is a much broader topic than information security alone.

The Information Commissioner's Office (ICO)[4] recommends the use of Privacy Impact Assessments (PIAs) as a structured approach for organisations to understand the privacy risks associated with the processing of personal data and take appropriate steps to manage those risks. PIAs are part of the ICO's Privacy by Design approach[5] that promotes privacy and data protection compliance from the start of any initiative.

Up to now, PIAs have been recommended best practice, and many organisations have found them to be a valuable tool. However, their adoption has been far from comprehensive.

With the GDPR coming into effect from 25 May 2018, this changes. There will be a statutory duty on organisations to undertake Data Protection Impact Assessments when using new technologies to process personal data in a way that is likely to result in a high risk to the rights and freedoms of individuals. Although the legislation is not clear on exactly what a Data Protection Impact Assessment will entail, it seems likely that a PIA will satisfy this requirement[6] and this document will assume that to be the case.

In effect, PIAs will become mandatory for some types of personal data processing.

In addition to any legal requirements, a PIA also shows that an organisation is concerned about data protection and often will help in other areas such as institutional audit.

1 *http://www.legislation.gov.uk/ukpga/1998/29/contents*
2 *https://ico.org.uk/for-organisations/data-protection-reform and http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN*
3 *www.ucisa.ac.uk/ismt*
4 *https://ico.org.uk*
5 *https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/*
6 *The Article 29 Working Party will produce guidance on this, see https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/whats-new/ and Article 29 Working Party archive http://ec.europa.eu/newsroom/article29/news-overview.cfm*

1.1 About this document

This Toolkit explains how to carry out Privacy Impact Assessments, and has been written specifically to meet the needs of the higher education community. A template for recording the outcomes of a Privacy Impact Assessment is also included.[7]

It builds on the more general guidance available from the Information Commissioner's Office[8], which readers are strongly encouraged to consult in addition to this document.

A companion document containing a worked example of a PIA for the introduction of Microsoft Office 365 at a fictional university illustrates how the process works, the type of privacy risks that a PIA can highlight, and the variety of solution approaches that might be available.

The author gratefully acknowledges the help of the Information Commissioner's Office and Microsoft UK in the preparation of this guide.

1.2 What is a Privacy Impact Assessment (PIA)?

A Privacy Impact Assessment is a structured approach for organisations to understand the privacy risks associated with the processing of personal data and take appropriate steps to manage those risks.

It is a process, not a report – although the resulting document will record the outcomes of the PIA as well as providing evidence that a PIA has taken place.

The 'deliverables' of a PIA include:

- a clear understanding of the privacy risks associated with the initiative in question;
- agreed measures to reduce those risks, where necessary, being built into the initiative;
- confidence among the stakeholders that any privacy issues have been addressed; and
- documentary evidence that the process has taken place.

The process comprises six distinct steps and a parallel stream of consultation. These are all explored in more detail later in the document.

A PIA need not be a lengthy exercise. In many instances, a PIA can conclude after the first step if it is determined that there are no significant privacy risks involved. Straightforward initiatives might require a full PIA, but this could be completed relatively quickly. More involved PIAs, such as the example used in this document (which covers a wide range of types of information, third party data processing and support for collaboration with external parties), could take significant time and effort.

1.3 Why conduct PIAs?

There are three key benefits to conducting PIAs:

- They give stakeholders confidence that the organisation is taking steps to safeguard their privacy, and a better understanding of how their personal data is being used. This in turn can lead to improved 'buy-in';
- They contribute to the success of projects by identifying issues early, when they are still relatively straightforward to address; and
- They are about to become a statutory requirement for some types of data processing.

In addition, the practice of conducting PIAs is an important contribution to general risk management within an organisation.

7 *Privacy Impact Assessment - Worked example for Office 365 www.ucisa.ac.uk/PIAOffice365*
8 *Conducting Privacy Impact Assessments Code of Practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf*

These benefits may best be realised by considering what can happen when privacy issues are not addressed in a structured, timely and transparent manner.

Consider the fictional[9] case study shown below.

> A university security service becomes aware of a personal safety app aimed specifically at university staff and students. It provides facilities such as incident reporting, pre-registration of valuables, first aid advice and mental health and wellbeing support. After discussion with the supplier and the accommodation department, it is decided to go ahead and offer the service. It is particularly attractive as, being a hosted service, the university does not have to develop or maintain any software or hardware, and new features are added all the time. The supplier is asked about security, and assures the university that there is no need to worry as the communications are all encrypted using https.
>
> The supplier brands the service to the university's requirements, and it is advertised on the university's website and in the literature given to all new students and particularly those staying in university-managed halls.
>
> Several months later, the university begins to receive complaints that students in some halls of residence are being targeted with advertising emails from local companies who seem to know a great deal about them. Once it is realised that only students who have registered for the safeguarding app have been affected, the university's Data Protection Officer is asked to investigate, and she in turn asks IT Services to help.
>
> It turns out that although the suppliers of the service were a UK company, the software itself was written by an Indian developer, and it is not immediately clear where the data are physically stored. The supplier didn't think that the data had been shared with any third parties (although the supplier's standard terms and conditions allowed them to do this), so they could not be sure whether they were the source of the information or if it had been 'hacked' by third parties unknown. They weren't aware of any such incidents, but would investigate both possibilities. Given the range of facilities available, the data stored about an individual could be very sensitive indeed, and the Data Protection Officer decides that all users of the service need to be informed, as well as the Information Commissioners Office.
>
> A local paper has got hold of the story, and presents it under the headline "University loses student mental health records."

A PIA would have soon identified the sensitive nature of the personal data being stored, and would have drilled down into the contractual, security and transparency issues at an early stage, thereby allowing this valuable service to be rolled out with much more confidence. Instead, the service had to be withdrawn, and the episode left the university with a damaged reputation.

1.4 Is a PIA needed?

Privacy Impact Assessments – at least the initial screening stage – should be undertaken for any initiative that involves the use of personal data, or any other activity that could have an impact on the privacy of individuals.

Very often this will mean a new computer system, or significant changes to an existing computer system. However, it could also be the implementation of new CCTV or other surveillance technologies or even the design of a new building for which glass-walled offices are being considered.

9 *Although the scenario is fictional, each of the elements has occurred in different institutions with different systems.* No criticism of any individual institution, service, product or supplier is implied.

Initiatives may be formal projects, perhaps governed by your institution's formal project management methodology. They could also be informal activities, perhaps a system upgrade to the latest version with new features, a student satisfaction survey or a major fundraising mailshot based on the data in the CRM[10] system.

Remember, if the initiative involves 'high risk' processing, a PIA is mandatory under Article 35 of the GDPR.

The first step in conducting a PIA is a screening process to decide whether the detailed work in the subsequent steps will be required. Therefore, when considering whether to conduct a PIA at all, it is safer to err on the side of caution, all that is at risk is the minimal effort to perform the screening in the first step.

1.5 When should a PIA be carried out?

Ideally, the PIA would be carried out in the early stages of an activity, as soon as a good idea of the data flows involved is available. In Prince2[11] terms, this would be during Project Initiation, or the first management stage.

Universities are accustomed to undertaking risk and impact assessments as part of any new initiatives, whether the assessments are for equalities, health and safety, or sustainability. Privacy Impact Assessments should be as much a part of the standard checklist as the others.

The later the PIA is conducted, the harder, and more expensive, it is likely to be to address any privacy risks identified, and the less effective it will be in addressing any concerns that stakeholders might have.

Having said that, it is never too late to conduct a PIA. A service might have been running for considerable time before it is realised that there could be privacy risks. A PIA carried out for an existing service would at least bring those risks to light and allow the organisation to decide how to manage them. Similarly, a PIA should be reviewed regularly and updated if new risks come to light.

Where an existing system involves 'high risk' processing you will need to undertake a PIA, unless you are able to demonstrate that the privacy risks have already been identified and addressed (for example by conducting a PIA at implementation), and that there have been no substantial changes to the processing since that assessment.

1.6 Who conducts a PIA?

The responsibility for conducting a PIA is something each institution will need to determine for itself.

Most universities will have a Data Protection Officer, and they will be well placed to have overall responsibility for PIAs. This should include maintaining a central register of all PIAs conducted, tools, training and awareness. However, while the Data Protection Officer may have overall responsibility for ensuring that PIAs are conducted and for providing advice and support to those doing them, PIAs will normally be undertaken by the relevant business area.

Responsibility for ensuring that individual PIAs are carried out may lie with the individual responsible for the project or service involved.

Anyone can conduct a Privacy Impact Assessment, however to be fully effective they need a sound appreciation of several areas:

- the information flows for the system under consideration;
- the nature of the technology employed;
- the principles of the DPA / GDPR;
- the consultation channels available within the institution to reach the stakeholders affected;
- the decision-making processes within the institution; and
- the institution's risk appetite.

10 Customer relationship management
11 A project management methodology

Clearly, the person conducting the PIA can turn to specialist support with any of these areas wherever necessary and the Data Protection Officer will be able to advise on many of them.

The PIA also has the potential to influence the costs, timescales and complexity of the initiative, so having the right level of management support is key.

2 Conducting a Privacy Impact Assessment

There are six steps to conducting a PIA:

1. Identify the need for a PIA
2. Describe the information flows
3. Identify the privacy and related risks
4. Identify and evaluate the privacy solutions
5. Sign off and record the PIA outcomes
6. Integrate the outcomes into the project plan

From Step Two onwards, it is important to consult with internal and external stakeholders as needed.

Each of these steps is described in more detail in the following sections.

2.1 Step One – Identify the need for a PIA

This step can be thought of as a screening stage.

The aim is to quickly discriminate between initiatives that have scope for privacy risks (and which therefore need the complete PIA), and those that do not.

Many activities clearly have no bearing at all on privacy matters, and would not even require screening. For example, a project to resurface a car park would require careful assessment in many respects, but privacy would not be among them.

Where there is any question at all, PIA screening should be undertaken. This would apply to the vast majority of information systems, CCTV roll-outs, automatic number plate recognition (ANPR) systems, anything involving payment other than by cash, physical access control systems and generally anything that involves identifying individuals.

In many institutions, the Data Protection Officer maintains a register of all PIAs undertaken. If this is the case, they should be notified that it is intended to screen the initiative.

In most cases, anyone with suitable knowledge and experience to undertake a PIA (see Section 1.6, Who conducts a PIA?) will find it easy to undertake this screening. Nevertheless, a set of screening questions can be useful as a prompt, and to standardise the approach.

A suitable set of screening questions is presented below. These are mostly drawn from the ICO's document *Conducting Privacy Impact Assessments Code of Practice* [12].

Will the project or its deliverables 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 which 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 which 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 particularly private.

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

Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?

Will the project involve the processing of personal data by third parties (third parties would include all cloud based services)?

Will the project expose personal data to elevated levels of security risks?

Are stakeholders likely to have privacy concerns about the project?

Your institution may want to add to this list.

If the answer to any of the screening questions is "Yes", then a complete PIA is likely to be needed, or at the very least a sound argument would need to be made for not undertaking one.

If an initiative seems to be borderline, it is better to be on the safe side and conduct the PIA.

A couple of examples below illustrate the screening considerations.

12 *https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf*

Screening example – a new Building Management System (BMS)

Your institution is implementing a new building management system for a refurbished set of lecture theatres and offices. The system uses passive infrared and motion detection sensors to turn off lights in unused rooms, and uses a feed from the University's timetabling system to decide when and which parts of the building needs to be heated and/or air conditioned. Information from the new system can be used to monitor room occupation.

As the system is not gathering any personal information at all, you might decide that there is no need even to undertake PIA screening. However, as the BMS has many sophisticated functions that might be used in future, you decide to err on the side of caution and screen.

The answers to all the screening questions turn out to be "No" and the project proceeds without a full PIA.

However, if at a later date the system were to be upgraded to also manage Access Control with personal access cards, or it was proposed to combine the room occupancy data for individual offices with information about who occupies which room, the situation would be substantially different and a full PIA would probably be required at that point.

Screening example – Office 365

Your university is planning the deployment of Office 365 to staff.

Office 365 is a 'hosted' suite of productivity and collaboration tools and is provided by Microsoft to its existing UK Higher Education customers from its datacentres in Europe (currently Dublin and Amsterdam, but with the possibility of moving to UK datacentres in the future).

Your students are already using many of the Office 365 facilities.

The project involves the processing of staff emails, calendar information, contact lists, tasks, notes, documents, conversations etc. in Office 365.

Because of the wide range of features in Office 365, and its role in supporting communication and collaboration, it is highly likely that it will be used for processing personal data.

Will the project involve the collection of new information about individuals? *There is a high likelihood that Office 365 could be used by individuals to gather personal data through the Forms feature for example.*

Will the project compel individuals to provide information about themselves? *No.*

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? *Because the service is hosted outside the UK by an American company, this would require further investigation, so impossible to say no at this stage.*

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? *No.*

Continued...

...continued

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. *No.*

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them? *No.*

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 particularly private. *It is possible that due to the nature of university services or research, information of this nature could be handled within Office 365.*

Will the project require you to contact individuals in ways which they may find intrusive? *No.*

Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support? *Yes, Office 365 offers the potential for file sharing with individuals outside the university and an online forms facility that could be used to gather personal data.*

Will the project involve the processing of personal data by third parties (this would include all cloud based services)? *Yes, Microsoft will be providing the data processing facility.*

Will the project expose personal data to elevated levels of security risks? *Yes, the facility will encourage the use of mobile devices and involve data transmission over the internet.*

Are stakeholders likely to have privacy concerns about the project? *Possibly, given the current political climate at least some groups in the university are likely to be concerned about the potential for external access to university information.*

If your institution requires it, inform the Data Protection Officer of the outcome of the screening.

If a PIA is not required, record the results with the rest of the documentation for the initiative. Otherwise, proceed with Step Two.

2.2 Step Two – Describe the information flows

This step involves a thorough analysis of the information that is to be processed.

The desired outcome of this step is to have a detailed description of the proposed information flows that is:

- sufficiently thorough to act as a solid basis for identifying potential privacy risks; and
- presented in a form that is comprehensible to the stakeholders.

At its simplest, this requires consideration of:

- what personal information is to be collected stored and processed;
- who will have access to it;
- what it will be used for;
- how long it will be kept and how it will be anonymised or deleted; and
- the assets on which personal data rely (hardware, software, people, paper, transmission channels).

In order to gather the necessary use case and technical information necessary for this step, it is likely that consultation with at least some of the stakeholders will be necessary. This is therefore the part of the PIA process where the consultation begins (see Section 2.7, Consultation).

This stage can be complicated by several factors, for example:

- the precise nature of the information, what it will be used for and the people who will have access to it could be quite open ended (the Office 365 example in this document is a good illustration of this);
- it might be necessary to take account of the potential for unintended access to the data, particularly if it is being stored, processed or transmitted outside the institution, or accessed through mobile devices; and
- the data might be used differently in the future to how it is expected to be used at the outset.

You should therefore be careful to avoid too simplistic representation of the information flows. Try to ensure that every aspect of the data gathering, storage, processing, transmission, analysis, sharing, archiving and disposal is accurately captured if it has a realistic potential for affecting the privacy of individuals.

Many projects will already have much of this information as a result of the analysis work necessary for the project design. If so, there is no need to re-invent the wheel.

There is no set format for presenting this information – the most appropriate form could be different for each project, but could include:

- narrative;
- process diagrams;
- other illustrations;
- any combination of these.

The information flows for an Office 365 implementation are illustrated in the companion document *Privacy Impact Assessment – worked example for Office 365* [13].

2.3 Step Three – Identify the privacy and related risks

This is in many respects the core of the PIA process.

The aim of Step Three is to compile a comprehensive list of all the privacy risks associated with the initiative, whether or not those risks require action by the project.

The PIA should concentrate primarily on privacy risks affecting individuals, although it would be sensible to include any risks that primarily affect the institution.

There is a temptation at this stage to include only those risks likely to have a material bearing on the initiative, and to exclude risks that have already been addressed in the proposed system.

For example, a project involving a new cashless payments element involves a risk that users card details could be 'hacked'. This risk should be included even though it has already been established that the service provider is PCI-DSS compliant. This will help guard against future changes accidentally removing the protection, in this case by recording that a PCI-DSS compliant service provider is a mandatory requirement.

Similarly, any risks identified by stakeholders during the consultation should be included, even if they turn out to be groundless. For example, a project to implement a new contactless access control system might solicit the concern that it could read private information on people's mobile phones. Although this concern may turn out to be based on a misconception about the technology involved, excluding it from the list of risks could be seen as undermining the process of consultation.

13 www.ucisa.ac.uk/PIAOffice365

Anyone who has engaged with the consultation process deserves to have their concerns listened to and addressed. The latter could take the form of anything from design/technology changes to documentation/messaging ones, see Section 2.4, Step Four – Identify and evaluate the privacy solutions.

This step requires considerable understanding and imagination to identify the less obvious risks, and the author of the PIA should be prepared for additional risks being highlighted during subsequent steps.

One approach is to start from the detailed description of the information flows, and consider the risks associated with each stage. Some people also find it useful to look at a set of privacy principles (e.g. the eight in the *Data Protection Act 1998*[14]), and seeing whether the proposed initiative *could* lead to a breach of any of them.

For each privacy risk identified there should be:

- a unique identifier;
- a short title;
- an explanation of the risk that is readily comprehensible by all the stakeholders;
- an assessment of the impact of the risk as it affects individuals;
- an assessment of the impact of the risk from a compliance perspective; and
- an assessment of the impact of the risk from the institution's perspective.

Many institutions will already have in place well developed approaches for managing risks within projects and at a departmental / institutional level. You should consider how to capture the risks identified as part of the PIA process in these other risk management frameworks.

As an example, the following risk could arise from a project to move from an in-house hosted student records system to the supplier's SaaS[15] offering.

Risk ID	SRS-PIA-007
Title	Data intercepted in transit
Explanation	Information entered into or retrieved from the student record system will need to traverse the internet between the user's PC or mobile device and the supplier's datacentre. This will involve transmission over parts of the internet over which neither the university nor the supplier have control. There is a risk that the information could be intercepted in transit, revealing personal information to third parties.
Impact on individuals	Personal, sensitive or confidential information may be used for unauthorised purposes or disclosed inappropriately.
Compliance impact	Organisation might be in breach of *Data Protection Act 1998* Principle 7 / *GDPR* Article 32.
Impact on organisation	Reputational damage, cost of defending prosecution, possible fines. University information may be used for unauthorised purposes or disclosed inappropriately.

In this example, the Risk ID has been allocated from the project or departmental risk register, thereby tying the PIA into the institution's risk management processes.

Note that at this stage, no information is provided about the solution to the privacy risk – that is the subject of the next step. The author of the PIA should be careful to ensure that the presentation of the output of this step (all the risks, but no solutions yet) does not unduly alarm readers. The template in Appendix A includes some reassurance on this point.

14 http://www.legislation.gov.uk/ukpga/1998/29/contents

15 Software as a Service – an approach where the supplier offers offsite hosting of the service and management of the software for upgrades, patches, capacity management etc.

2.4 Step Four – Identify and evaluate the privacy solutions

This is where solutions are identified for the risks.

The aim is to identify, for each of the privacy risks listed in Step Three, sufficient solutions to eliminate the risk or reduce it to a level that is acceptable by the institution.

For some identified risks, no solution is required because the likelihood is so low or the impact so small that it is already acceptable to the organisation. Most identified risks, however, will need some action to eliminate or render them acceptable, and in some cases, there could be more than one solution identified.

Continuing the example in Section 2.3, Step 3 – Identify the privacy and related risks:

Risk ID	SRS-PIA-007
Title	Data intercepted in transit.
Solution(s)	The supplier's datacentre has a direct connection to the Janet network. The traffic between the client device and the servers is encrypted using https.
Action Required	None.
Effect	The risk is reduced to the level where it is accepted.

The solutions here illustrate three points:

- The supplier's direct connection to the Janet network will certainly reduce the likelihood of traffic interception between on campus users and the datacentre, and because this is the most common use case, the solution is good news. However, it will do nothing to prevent interception for off-campus users, as they will be using other networks. This demonstrates the importance of having a thorough understanding of the use cases and information flows.
- The use of https encryption might be thought of as eliminating the risk altogether. Certainly, given the current state of technology, it would reduce the risk to a very low level indeed. Whether or not this counts as eliminating it entirely is for the author to decide.
- Neither of the identified solutions requires the institution to take any action – both are 'built in' to the proposed system. Not all privacy solutions require actions to be added to the project plan.

The solutions may take many forms, for example:

- No solution necessary – the risk is based on a misconception[16] or is so unlikely to be realised (or so minimal in impact) that it is acceptable with no further action.
- A contractual arrangement between the supplier and the institution will provide the additional assurance necessary.
- A fair processing notice and opt-in approach can inform users about how their data will be used and give them the opportunity to positively record their agreement to participate.
- A policy can be introduced to reduce the risk to an acceptable level.
- Operational procedures might be introduced to manage the risk.
- Certain features in the product can be disabled.
- A training programme could be deployed to make people aware of the risk and the actions to take to avoid it.
- Technical measures, such as the enforced use of strong encryption, could be built into the project to reduce the risk.
- As a last resort when no other solutions are available, the initiative may have to be abandoned as involving too high a risk for the organisation to accept.

16 Although if others are likely to share the misunderstanding, a mitigation involving improved communication would be advisable.

The solutions identified need to be acceptable to the institution, both in terms of reducing the risks to acceptable levels and in terms of not fatally undermining the business case for the initiative. The solutions will also need to be acceptable to all the other stakeholders.

Remember that for each risk, it may be appropriate to deploy several solutions in parallel.

2.5 Step Five – Sign off and record the PIA outcomes

This step is where the proposed solutions are formally approved.

The aim is for an appropriate individual or group with the authority to speak on behalf of the institution, to confirm that the combination of proposed privacy solutions eliminates the risks or reduces them to levels that the organisation accepts, and to record the fact.

Identifying this appropriate person or group is a matter for the institution to decide. It will depend on the governance structures in place and the institution's attitude to risk.

Suitable people might include:

- the project executive or sponsor;
- the data protection officer;
- the director of the area 'owning' the initiative;
- the university secretary / registrar / Clerk to Board of Governors; or
- the chair of an appropriate committee.

Whoever signs off the solutions should have a clear understanding of the initiative, and in particular what the privacy risks are and how the solutions address them.

There should be a permanent record of who signs off the solutions and when this took place.

2.6 Step Six – Integrate the outcomes into the project plan

This is where the required actions identified in Step Four are built into the plan for the initiative.

The aim is to ensure that where an agreed solution requires something to be done, there is a clear plan of action to do it, together with a named person responsible for making it happen.

Remember that not all solutions to privacy risks require actions – some may already be 'built in' to the initiative.

In the case of formal projects, many of the required actions will be within the scope of the project, so they are managed in the same way as any other project task. Effort is estimated, resources assigned, dependencies identified, the task is scheduled and progress is monitored.

Other actions will be beyond the scope of the project (for example, a change to a university policy). These will need to be assigned through the normal management processes and added to the list of project dependencies.

For initiatives being run as informal projects or business-as-usual activities, the normal management processes should be used to identify who will undertake the work, when it will be done and how the team will be kept informed of progress.

In all cases, the name of the person responsible for each action together with the timescale for completion should be permanently recorded.

In the absence of any other project management documentation, the PIA documentation would also be a good place to record when the action has been completed.

2.7 Consultation

Consultation with the stakeholders can take place throughout the PIA process, although it is usual to wait until the need for a PIA has been confirmed.

Step	Activity	
One	Identify the need for a PIA	
Two	Describe the information flows	Consultation
Three	Identify the privacy and related risks	
Four	Identify and evaluate the privacy solutions	
Five	Sign off and record the PIA outcomes	
Six	Integrate the outcomes into the project plan	

Consultation serves many purposes throughout the PIA process, for example to:

- explain to stakeholders what the initiative is;
- explain to stakeholders how the PIA process will be used by the initiative to manage the privacy risks;
- establish what the current working practices are that the initiative aims to update or replace;
- find out how the new system or process is likely to be used in practice, and in the case of general-purpose facilities, what they are likely to be used for;
- find out what privacy concerns the stakeholders have;
- solicit suggestions for solutions; and
- explain to stakeholders what privacy solutions have been identified.

Note that consultation addresses many stages in the PIA process.

Note also that consultation is a two-way street. It is as much about gathering information as it is about sharing information. Consultation can often throw up both privacy risks and solutions that would otherwise have been missed.

This range of purposes should give some idea of the range of stakeholders who might need to be involved:

- the people who understand the initiative and any predecessors from a technical and information point of view;
- the people who will be using the new system;
- the people whose information will be processed by the new system;
- the people who have responsibility for data protection and information security within the institution;
- collaborative partners; and
- the suppliers of a system.

Some of these groups might be difficult to reach.

For example, the people whose information will be processed by a new system could be a large, as yet unidentified set of people outside the institution. Their interests might best be represented by the institution's data protection officer and a carefully constructed fair processing notice. For some initiatives, the research ethics committee may have a valuable role to play here. Focus groups may be useful if particular groups of people outside the institution can be identified and contacted. For particularly complex cases, advice should be sought from the Information Commissioner's Office.

Other groups that can often be challenging to reach are the students and staff, who could be both users of the system and data subjects. Several approaches might be applicable:

- involve the Students Union and/or staff union representatives in the consultation process;
- identify some key users and involve them (although you need to be clear whether they are acting in a personal capacity or representing the wider body);
- invite participation through an institution-wide mailshot;
- invite participation through faculty / departmental / course leaders; and /or
- use existing committee structures.

The most appropriate combination will depend on what the initiative is and what channels of communication are most effective in your institution.

It is recommended practice to publish the findings of the PIA, and this can be thought of as the culmination of the consultation. Unless there is good reason not to, the PIA should be publicly available. However, the PIA could contain some sensitive material so either the appropriate material should be redacted in the more widely available versions, or the circulation could be restricted. Depending on the level of interest in the initiative, publication could be simply posting the PIA on a web site, it could be an institution-wide email or it could be one or more presentations or appearances at relevant committees or groups.

Remember that one of the benefits of conducting Privacy Impact Assessments is that they give stakeholders confidence that the organisation is taking steps to safeguard their privacy, and a better understanding of how their personal data is being used. This in turn can lead to improved 'buy-in' for the initiative.

If the consultation is not carefully planned and executed, this benefit is lost.

3 Conclusion

The Privacy Impact Assessment is a simple yet powerful tool to ensure that privacy risks are identified early in a project while it is still relatively easy to do something about them. The approach ensures that the identified solutions are formally accepted by the institution, and translated into specific actions that are built into the project.

Consultation throughout the process ensures that as much information as possible about the privacy risks is captured and disseminated, building confidence among the stakeholders that this aspect of the initiative has been well thought through.

We hope you find this Toolkit, the accompanying template and the worked example to Office 365[17] useful and wish you every success in your adoption of Privacy Impact Assessments.

17 Privacy Impact Assessment - worked example for Office 365 www.ucisa.ac.uk/PIAOffice365

4 A Privacy Impact Assessment Template

The following template is suggested for recording a Privacy Impact Assessment. You may well need to modify it slightly to meet the needs of your institution.

[Initiative] – Privacy Impact Assessment

This document records the outcome of a Privacy Impact Assessment for [the initiative] at [institution].

It follows the approach recommended by the UCISA Privacy Impact Assessment Toolkit and the Information Commissioner's Office Code of Practice.

[A brief introduction to the initiative – What is it? Who is it going to affect? When is it likely to happen? Does it replace or update something people are already familiar with?]

Step One – Identify the need for a PIA

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 which 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 which 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 particularly private.

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

Will the project introduce new facilities that might be used by individuals in the institution to gather, process, analyse or share personal information in ways that would previously have required specialist support?

Will the project involve the processing of personal data by third parties (third parties would include all cloud based services)?

Will the project expose personal data to elevated levels of security risks?

Are stakeholders likely to have privacy concerns about the project?

Based on the above information, it has been decided that a full Privacy Impact Assessment [is/is not] required.

Step Two – Describe the information flows

[Give a detailed description of the information to be processed, how it is processed and how it flows. See Section 2.2. Step 2, Describe the information flows]

Step Three – Identify the privacy and related risks

"Table 1 – Privacy risks and their explanation" lists the potential privacy risks identified from the changes to the information flows outlined above, and provides an explanation for each one, describing how the risk arises. "Table 2 – Impact of privacy risks" examines the potential impacts should these risks materialise.

Note that this list includes all the identified risks, rather than just those that are likely to require action to be taken. **Solutions for all these risks are identified later in this document.**

Risk ID	Title	Explanation

Table 1 – Privacy risks and their explanation

Risk ID and Title	Impact on individuals	Compliance impact	Impact on institution

Table 2 – Impact of privacy risks

[Note: depending on the complexity of the risks identified, it may be possible to combine these tables into one.]

Step Four – Identify privacy solutions

This step involves examining each of the risks identified in Step Three and identifying solutions that will bring the residual risk to a level where the university can accept it.

In some cases, these solutions are inherent in [initiative], and no further actions are required. In other cases, further action will be required and these will need to be integrated back into the project plan (see Step Six).

To avoid repetition, the information for Steps Four and Five have been consolidated into "Table 3 – Risks, solutions, and acceptance". Columns one two three and four of this table record the outcomes of Step Four. For convenience in Step Six, column three records any specific actions required to implement the solutions identified.

Step Five – Sign off and record the PIA outcomes

Whether the solution to a privacy risk involves taking additional action or not, the university needs to formally consider the risk and the proposed solution, and satisfy itself that the residual risk had indeed been reduced to an acceptable level.

Step Five records the formal acceptance of the residual risks by appropriate people on behalf of the university.

Column five of "Table 3 Risks, solutions, and acceptance" records the outcomes of Step Five.

Risk ID and title	Solution(s)	Action Required	Result: Is risk eliminated, reduced or accepted?	Approved by

Table 3 – Risks, solutions, and acceptance

[Note that you may need to be flexible in how you use the table. A risk may have multiple solutions, a solution may have more than one action, and several risks could share the same solutions and actions.]

Step Six – Integrate the outcomes into the project plan

The agreed actions need to be built into the project plan. This involves identifying a date by which they will be completed, and the name of the individual responsible for their completion.

Table 4 – Action Plan, records the outcomes of Step Six. Note that those privacy risks for which no actions are required are omitted from this table.

Risk ID and Title	Action Required	Date for completion	Responsibility for Action

Table 4 – Action Plan

Consultation

The conduct of this Privacy Impact Assessment has involved the following consultation:

[A summary of the consultation, specifying the channels used for consultation and naming groups. Committees, external organisations and individuals where appropriate. Be particularly careful to include records of advice being taken from the Data Protection Officer, and consultation with data subjects where this has taken place.]

5 Acknowledgements

Lead author

Jerry Niman, Jerry Niman IT Services

Anna Mathews, UCISA Head of Policy and Projects was the project manager for this publication. We are grateful to the following people for their helpful comments in the preparation of this document:

Victoria Cetinkaya, Senior Policy Officer (Public Services), Information Commissioner's Office

Stuart Aston, National Security Officer, Microsoft UK

Advisors and critical friends

We are appreciative of the assistance received from colleagues across the sector. In particular, we would like to thank the following individuals who were involved in early discussions about the Toolkit, who provided information, or acted as critical friends during the drafting process:

Sally Beauchannon, IT Business Relationship Manager, Royal Holloway, University of London

Paul Butler, Director of Information and Library Services, University of Greenwich

Andrew Cormack, Chief Regulatory Adviser, Jisc

Anthony Cotton, Information Assurance Officer, University of Derby

Ceri Davies, Head of IT Architecture, Cardiff University

David Hayling, Head of IT Infrastructure, University of Kent

Peter Hurst, Head of Communications and Collaboration Services, Lancaster University

Rachael Maguire, Records Manager, London School of Economics

Simine Marine, Serials/Systems Librarian and Data Protection Officer, Architectural Association School of Architecture

Aldo Maugeri, Information Governance Manager, University of Canterbury

Kathy McCabe, University Librarian and Director of Information Services, University of Stirling

Shane Murphy, IG Consultant, St George's, University of London

Dee Ogunjobi, Director of CIS and IT Services, RACC and Hillcroft Federation

Peter O'Rourke, Director of IT, University of Suffolk

Helen Rishworth, Information Governance Manager, University of Derby

Ian Robotham, Medi-CAL Unit and Academic Applications Development Manager, University of Aberdeen

David Sharkey, Information Security Manager, Keele University

Rob Stockton, Head of Learning Resources and Information Systems, Wrexham Glyndwr University

Darren Tysoe, Chief Information Officer, Regent's University London

Fiona Wheater, Senior Policy, Planning and Governance Officer, University of Stirling

Mike Whyment, Program Manager, IT Services, University of Aberdeen

Gavin Wiltshire, IT Security Officer, University of Kent

6 Copyright, disclaimer and availability

Copyright

Disclaimer

Availability

The UCISA Privacy Impact Assessment Toolkit and the UCISA Privacy Impact Assessment – Worked example for Office 365 is freely available to download for non-commercial use from www.ucisa.ac.uk

Universities and Colleges
Information Systems Association

University of Oxford
13 Banbury Road
Oxford OX2 6NN

Tel: +44 (0)1865 283425
Fax: +44 (0)1865 283426
Email: admin@ucisa.ac.uk
www.ucisa.ac.uk