Data Protection Handbook

Contents

1 – Introduction

The UK General Data Protection Regulation and the Data Protection Act 2018 cover all personal data processed by the University, irrespective of where the data is held and what format it is held in.

2 – Glossary

The following terms are used within the Data Protection Handbook and the guidance documents:

The UK GDPR – UK General Data Protection Regulation

The DPA – Data Protection Act 2018

Personal Data – Current data protection legislation applies only to personal data about a living, identifiable individual.

Special Categories of Personal Data – Personal data is classed as belonging to "special categories" under current data protection legislation if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin
- political opinions
- religious beliefs
- trade union membership
- physical or mental health
- sexual life or sexual orientation
- commission of offences or alleged offences
- genetic data
- biometric data

Please note the new guidance on genetic data on the website.

Data Subject – A data subject is an individual who is the subject of personal data.

Processing – Data processing is any action taken with personal data. This includes the collection, use, disclosure, destruction and holding of data.

Data Controller – A data controller is an organisation that has full authority to decide how and why personal data is to be processed, and that has the overall responsibility for the data. This includes deciding on use, storage and deletion of the data.

Data Processor – A data processor is an organisation that processes personal data on behalf of another organisation.

Automated Decision-Making – Automated decision-making takes place where decisions are made solely by automated means without any human involvement.

Profiling – Profiling means automated processing of personal data to evaluate certain things about a person, in particular to analyse or predict aspects concerning that person's performance at work, economic situation, health, personal preferences, reliability, behaviour or movements.

The detailed definitions can be found here:
Definitions

3 – Key considerations

Before embarking on any processing personal data, whether that be sharing personal data with a third party, using a new online tool, marketing a new programme or any other action that involves the use of personal data, you should ask yourself the following questions:

- Do you really need to use the information? Are there alternative ways the same objective can be achieved without using or sharing personal data?
- Could anonymised or pseudonymised data be used?
- Do you have a valid justification for processing the data e.g. it is required for a contract or has the data subject given their consent? (see section 6)
- Has the data subject been told about the processing i.e. been issued with a privacy notice? (see section 5)
- Are you sure that the personal data will be secure during the process? (see section 4)
- Are you planning to pass personal data on to a third party or transfer the data outside the UK or EEA? If so do you have the necessary safeguards/ permissions in place to do this? (see section 10)
- If you are setting up new systems/processes, have the Data Protection by Design and Data Protection Impact Assessment guidelines been followed? (see section 15)

If having considered the points above you conclude that the processing of personal information is necessary, then the information in the following sections will provide more details about the factors that need to be considered and the actions that need to be taken to ensure the processing meets the requirements of UK GDPR and the DPA.

4 – Data Security

The Information Security Directorate, led by the University Chief Information Security Officer (CISO), is responsible for leading and maintaining the University information security risk strategy. They encourage a holistic approach to managing information security risks and lead pan-University information security initiatives, providing strategic advice on existing and emerging information security threats. They also deliver security awareness training across the University through regular general awareness sessions and provide bespoke sessions when required.

On the Information Security website, you will find details of the information security risk management framework, together with other useful information to help you protect the information you process appropriately. You will also find details about the mandatory information security training you must complete.

Detailed guidance on data security can be found here:
Information Security

5 – Privacy Notices

Under the 'fair and transparent' requirements of the first data protection principle, the University is required to provide data subjects with a privacy notice to let them know what we are doing with their personal data.

A privacy notice must be:

- easily accessible,
- provided at the time of collecting the data,
- written in a clear and concise way

The University uses a layered approach to privacy notices: The first half of the privacy notices is provided directly to the data subjects. This first half includes all the information that needs to be customised (purpose, legal basis, recipients, retention times, automated decision-making, international data transfer). At the bottom of this first half is a link to the second half which contains the information that is generic to all data processing (contact details of the DPO, data subject rights, rights to complain to the ICO), which is located on a website. The purpose for this approach is to make the privacy notice provided to data subjects as short and easily readable as possible.

The University privacy notices can be found here:
University Privacy Notices

Where personal data is collected outwith these two situations, a separate privacy notice will be provided by the College/School/Department collecting the data. Examples are conference registration, newsletters, student applications directly to a School.

A template for privacy notices and guidance on how to complete the template is provided here:

Privacy Notice Template

6 – Lawfulness

Whenever the University processes personal data in any way, there must be a valid justification, a so-called legal basis (also called 'lawful basis') for doing so. The UK GDPR and the DPA provide a list of six legal bases for personal data. If special categories of personal data are processed, the law provides an additional list of legal bases. Thus, for special categories, one legal basis from each of the two lists must be met.
The legal bases to choose from for personal data are:

- consent
- necessary for performance of a contract
- legal obligation
- vital interest
- necessary for the performance of public tasks/core functions
- necessary for a legitimate interest.

If you decide to use 'necessary for a legitimate interest' as your legal basis, you will have to conduct a Legitimate Interest Assessment ("LIA"). To be assigned an assessment, contact the DPO at dpo@ed.ac.uk . To find out whether an LIA has already been conducted, you can view all completed LIAs here:
Completed LIAs

For special categories of personal data, the relevant legal bases for the University are:

- explicit consent
- necessary for purposes of employment or social security law
- necessary for reasons of substantial public interest
- necessary for medical purposes
- necessary for archiving purposes or statistics and research.

A full description of these legal bases together with examples for their use can be found here:
Guidance on Legal Basis for Processing

7 – Retention

The UK GDPR sets a clear requirement for the University to take its data retention responsibilities seriously. Generally, personal data should only be retained for as long as necessary. Just how long 'necessary' is, however, can differ based on the type of data processed, the purpose of processing or other factors. Not only do you have to inform data subjects in the privacy notice how long you keep their personal data for, you will then have to ensure that these retention times are adhered to. This means that data will need to be deleted, destroyed or fully anonymised at the end of the retention time or archived appropriately in the University Archives.

It is important to note that on the other hand, in some circumstances personal data must be kept as destroying such data would be a data protection breach, for example the core archival student record to verify a student's qualifications.

Data retention is a personal responsibility for everybody in the University and it is important that you have an overview of where personal data is stored. This may include:

- own servers
- third party servers
- email accounts
- Sharepoint sites
- OneDrive accounts
- Teams chats
- Shared drives
- backup storage
- paper files

Wherever possible, University Services and hardware should be used to store University records. The University's core systems should predominantly be used, as part of a departmental filing scheme where necessary; records should not be stored within the internal storage of individual computers. For example, you should not run reports and save them in spreadsheets in a folder on your desktop. Systems must be set up to make this less likely to happen in the first place. Staff should use managed desktops or connect remotely where practical.

To determine how long to retain a document containing personal data, first consult the relevant privacy notice. If the detail you require is not contained in the privacy notice, consult your business unit's data processing register. The registers can be found in Sharepoint:
Data Processing Registers

8 – Data Sharing

You may be asked to share personal data both within the University (by colleagues in your own area or in another unrelated area) and outwith the University (by another organisation). Note that if you use an external company or organisation to process personal data on your behalf (a 'data processor'), the requirements for data sharing do not apply.

Internal data sharing
Internal data sharing, whether with a colleague from your own area or somebody from another unrelated area will usually be unproblematic as long as a data access protocol is completed and approved by the respective data steward. There are two types of data access protocols, one for one-off, ad hoc data sharing requests, and one for APIs or regular data dumps. The type of questions the protocols contain are:

- Would data subjects reasonably expect their data to be shared with you and is the purpose for sharing the data consistent with what the data subjects have been told in the privacy notice and do the legal basis and retention periods still apply? Would data subjects reasonably expect their data to be shared with you? The key privacy notices can be found here:
    - Staff privacy notices
    - Student privacy notices

- Has a Data Protection Impact Assessment been carried out – if not, why not? (see section 15)
-

External data sharing

If another organisation requests that you share personal data, then you will need to ask these questions:

- Does the sharing involve the transfer of data outside the UK or the EU? (see section 10)
- Is the third party acting as a processor for the University i.e. acting under the instruction and on behalf of the University?
- Is the third party requesting the personal data for their own use and purpose? Then the third party is another data controller.

If you are setting up a relationship with an outside organisation that will involve the transfer of personal information, you must put in place a contract to ensure that adequate protection is given to that information so that the University meets its data protection obligations and protects the rights of the individuals involved.

There are specific contract requirements depending on the circumstances. For example, the standard terms and conditions of most cloud service providers are not normally sufficient. The University's Legal Services Team and/or IS can provide template agreements to meet the needs of different transfer arrangements. They can be contacted at:

legalservices@ed.ac.uk

and/or

informationsecurity@ed.ac.uk

9 – Third Party Requests

The University often receives requests for the personal information of its students and staff from third parties. Detailed guidance on sharing personal data with third parties can be found here:

Sharing Personal Data

Requests from parents, friends or relatives of a student

No release without the student's consent.

It is acceptable to advise the requesters that we will accept a message and, if having checked our records and such a person exists, will pass it on. This avoids disclosing any information about the student, including whether or not they are at the University.

More guidance can be found here:

Parents and Family Members

Requests from organisations providing financial support

The University routinely notifies public funding bodies and the Student Loans Company of changes to a student's status. These disclosures are covered in our privacy notices and records of processing activities. Records should not be disclosed to organisations that are not covered in our privacy notices (e.g private funders) without evidence of student consent.

Requests from Home Office/UK Visas and Immigration (UKVI)
The University often receives requests for information on attendance and other details relating to international students. Information should only be disclosed where we are satisfied there is a legal requirement to provide the requested information or the individual concerned has given their consent. Requests for student information should be passed on to the Immigration Compliance Team

Requests from the Police or law enforcement officials
The University is not legally obliged to provide information to the police, unless presented with a court order. However, the University will usually choose to release information where the police, or other law enforcement agencies, can demonstrate to our satisfaction that non-release would be likely to prejudice the prevention/detection of crime or apprehension/prosecution of offenders.
For such requests, the established procedure can be found here:
Police enquiries, and similar agencies

The University may receive requests for information regarding an allegation of fraud or misrepresentation as regards degree results. For such requests, guidance can be found here:
Fraud or misrepresentation

Disclosures required by law
There are circumstances where the University is legally obliged to disclose information about an individual to a third party if this is required by law, enactment or court order:

Third Party	*Authorisation for disclosure*
UK Funding Councils e.g. HEFCE HEFCW, SFC and their agents e.g. QAA, HESA, HEFCE auditors	Further and Higher Education Act, 1992 s.79
Electoral registration officers	Representation of the People Act 2000; The Representation of the People (Scotland) & (England and Wales) Regulations 2001
Officers of the Department of Works and Pensions, and Local Authorities	Social Security Administration Act 1992: s.110A, s.109B and s.109C
Health and Safety Executive	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013 s.3
Audit Commission and related auditing bodies	Audit Commission Act 1998 s.6
Environmental Health Officers	Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988
Environment Agency	Agency Regulations – specific ones to be quoted
Inland Revenue	Taxes Management Act 1970
Other third parties	With a Court Order

With such requests, we must ensure that any legal obligation (details of legislation and relevant section) is correctly described by the requestor in writing.

10 – Data Transfer Outside the UK

International data transfer can be:

- Sending personal data from the University to an organisation, company or an individual that is based in a non-EEA country such as during research collaborations, for student exchange or using external examiners
- Uploading photos of identifiable individuals to a University website

These transfers are not prohibited, however, we must ensure that so-called safeguards are in place and we must conduct a Transfer Risk Assessment (TRA). The TRA is included in the DPIA, however, if no DPIA is required, a separate TRA is available from the DPO. An assessment of countries that the University engages with regularly for student exchange has been conducted and the DPO will assist with any TRAs.

The UK GDPR provides a list of these safeguards, one of which must apply:

Adequacy of the country: The EU has assessed the third country to have an adequate level of protection. These countries are then treated as though they were an EU member state and data can be transferred there without the need for any further safeguards. The countries that currently fall into this category are:

- Andorra
- Argentina
- Canada
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- Faroe Islands
- Japan

The EU has made an adequacy decision in favour of the UK, so data transfer between the UK and the EU is unrestricted.

Transfers to the USA: The EU has created a Data Privacy Framework together with the USA. The UK has taken that on board and created an additional Data Bridge between the UK and the USA. Data controllers who wish to export data to the USA will need to ensure that the American data recipient has a) signed up to the Data Privacy Framework and b) subsequently to the Data Bridge. If the recipient has done neither, an International Data Transfer Agreement is required.

International Data Transfer Agreement: Two contractual transfer mechanisms can be used to send personal data abroad: the International Data Transfer Agreement (IDTA) and the International Data Transfer Addendum to the European Commission's Standard Contractual Clauses (Addendum). Information and templates of these mechanisms can be obtained from Legal Services at: legalservices@ed.ac.uk. Additionally, a risk assessment must be completed and approved by the DPO. This risk assessment is contained in one of the questions in the DPIA.

Court orders: You have received a court order requiring the transfer.

Consent: The data subject has given explicit consent to the transfer, having been informed of the possible risks of such transfers due to the absence of an adequacy

decision and appropriate safeguards. Where transfers are done on the basis of consent, evidence of the consent and when it was obtained should be kept.

Contract with the data subject or in the interest of the data subject: The transfer is necessary for a contract between the data subject and the University, for example when non-EEA students ask for their exam results to be sent to their funding organisation in their home country. When students wish to spend a term abroad, there will be a contract between the University of Edinburgh and the host university and that contract is in the interest of the students.

Public interest: The transfer is necessary for important reasons of public interest. Examples for this are crime prevention and detection, or national security.

Lawsuits: The transfer is required for a lawsuit.

Medical emergencies: The transfer is necessary for a medical emergency.
Staff authorising transfers of personal data outside the EU are responsible for ensuring that one of the above requirements is met and ensuring that a record is kept of which safeguard is in place.

For more advice on transfers of personal data outside the EU please consult the guidance:
International Transfer Guidance

11 – Data Subject Rights

The UK GDPR lists eight data subject rights that the University will need to comply with, these are the rights of the data subject to:

- Be informed
- Subject access
- Erasure (to be forgotten)
- Rectification
- Portability
- Object
- Restrict processing
- Object to automated processing and profiling

Right to be informed: The right to be informed is complied with by issuing a privacy notice, please see Section 5.

Subject access right: The purpose of subject access rights is to allow individuals to obtain a copy of their own personal data, confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of correction or objection if necessary. The University must respond to all requests for personal information within one month. Any member of staff receiving a request from an individual for their own personal information should consult the relevant guidance on the Information Compliance Services website:
Dealing with Subject Access Requests

Right to erasure (to be forgotten): Data subjects have the right to request that their personal data be removed from all the systems of the University if certain requirements are met. These requirements are:

- The University does not need to keep the data anymore in relation to the purpose for which they were originally collected/processed.
- The data subject withdraws consent for the processing to which they previously agreed
- The subject uses their right to object to the data processing (possible where the legal basis is either 'public task' or 'legitimate interest').
- The University is processing the data unlawfully (i.e. in breach of the UK GDPR and/or the DPA)
- The personal data must be erased in order to comply with a legal obligation.
- The data subject was a child at the time of collection.

This means that if the legal basis for processing the data is 'performance of a contract' or 'legal obligation', and processing is fully lawful, the request must be refused.

However, even if the request meets one or more of these requirements, there are still a number of exemptions when the University will not have to comply. Thus, data might not have to be erased if any of the following apply:

- The personal data are processed to exercise the right of freedom and expression (e.g. journalism, artistic work)
- The personal data are needed for legal compliance
- There are reasons of public interest in the area of public health
- The data are processed and stored for scientific, historical research or archiving purposes in the public interest
- The data are needed for a lawsuit

Right to rectification: Data subjects are entitled to request that their personal data are rectified if the data are inaccurate or incomplete. If you receive such a request, you must comply within one month. Should complying with the request for rectification be particularly complex, then the time can be extended to two months.

If you have shared the personal data with third parties, or within the University, you must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort.

Right to portability: The right to data portability gives data subjects the possibility to request that the University pass their personal data on to a third party of their choice and allow that third party to import the data automatically.

Data subjects have this right if certain requirements are met. These requirements are:

- The individual has provided the personal data to the University, and
- The legal basis for processing is 'consent' or 'performance of a contract', and
- The processing is carried out solely by automated means with no human involvement.

If these requirements are met, then the data must be provided in a structured, commonly used and machine readable form.

Right to object: Data subjects have the right to object to the University processing their personal data if certain requirements are met. These requirements are:

- The legal basis for processing is 'legitimate interest' or 'public task';
- Direct marketing (including profiling); and
- Processing for purposes of scientific/historical research and statistics.

When data subjects have an objection on "grounds relating to his or her particular situation", then you must stop processing the personal data unless:

- You can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or
- The processing is for the establishment, exercise or defence of legal claims.

The right to object to profiling for direct marketing is an absolute right. That means that for such objections, data subjects will not need to provide any grounds relating to their situation, and the University is not allowed to override the objection.

Right to restrict processing: Data subjects have a right to 'block' or suppress processing of their personal data, i.e. to request that you immediately stop processing their personal data in any way except to store it. This right applies only if one of these requirements are met:

- A data subject contests the accuracy of the personal data - you should restrict processing until you have verified the accuracy.
- A data subject has objected to the processing (see above), and you are considering whether the University's legitimate grounds override those of the data subject.
- Processing is unlawful, the data subject does not trigger the right to be forgotten, but requests restriction of use instead.
- You no longer need the personal data and would delete them in accordance with the retention schedule, but the data subject requires the data for a lawsuit.

If you receive a request for erasure, rectification, portability, restriction or an objection to processing, immediately contact your local Data Protection Champion.

A list of the Data Protection Champions can be found here:
Data Protection Champions

Right to object to automated processing and profiling: see section 14 on automated processing and profiling

12 – Research

Research is governed by data protection legislation if it contains personal data or pseudonymised data. Data are personal if a piece of information directly identifies

individuals or, if viewed in combination with other bits of information you have access to (or that you know), you could identify individuals.

Data are pseudonymised if you remove all direct identifiers from the research dataset, attribute a study specific identifier to each individual, and keep a link between both.
A dataset is truly anonymous when you can no longer identify an individual directly from the information combined with information that is available by other means or from other sources. This involves consideration of all of the means reasonably likely to be used to identify an individual without going to great effort.

Research under the UK GDPR will require informed, voluntary ethics consent to participate in a study, as well as a Participant Information Sheet.

The legal basis for processing personal data will be 'public task' and for special categories of personal data, 'necessary for scientific or historical research purposes in accordance with safeguards'. These safeguards are what is currently considered good practice:

- The minimisation principle – use only the absolute minimum of personal data required for your purpose
- Anonymise personal data if you can
- If you cannot anonymise, wherever possible, pseudonymise all personal data
- Store the data securely

Furthermore, you must be able to prove that research is in the public interest. Possible evidence includes one of the following:

- Your research must be proportionate,.e.g. it must not be more intrusive into participants' privacy than necessary, you must not collect more data than you actually need for your study
- Your research is subject to a policy research governance framework, e.g. the UK Policy Framework for Health and Social Care Research
- Research Ethics Committee (REC) review (does not have to be a European REC)
- Peer review from a research council
- In the case of medical research, Confidentiality Advisory Group (CAG) recommendation for support in England and Wales or support by the Public Benefit and Privacy Panel for Health and Social Care in Scotland.

When you have the necessary safeguards in place, the rights of research participants can be restricted. It will be up to the individual Principal Investigator's discretion whether the following rights should not apply where it would prevent or seriously impair the achievement of the research purpose and where your legal basis is public interest plus the additional research-related legal basis for special categories:

- The right to rectification
- The right to restrict processing
- The right to object to processing
- The right to erasure (right to be forgotten)

If your research involves collaboration with an industry partner, your legal basis will be 'legitimate interest'.

More detailed guidance can be found here:
Research under UK GDPR

13 – Student Research

Students will conduct research as part of their undergraduate work (Honours dissertation) or as part of their postgraduate work (dissertations for a Masters Degree or a Doctorate). Students will remain the data controller and as such responsible for their research until they submit their dissertation. However, as students work strictly on behalf of themselves in order to achieve a degree, this processing activity falls under what used to be called the domestic uses exemption, which means that data protection legislation does not directly apply. However, students will be bound by the University's policy and procedures due to the Student Contract with the University. Thus, the Data Protection Policy applies to students processing personal data as part of their work to pursue a course of study and they will be required to ensure that their work is compliant. They will also be required to conduct a data protection impact assessment as part of their Ethics Approval. The data protection impact assessment will be reviewed and approved by their supervisor.

Once the dissertation is submitted, the University becomes a joint data controller with the student.

The only exception to this is where a student processes personal data whilst working on a project led by a university research group. In this case, the student and the University are both data controllers from the outset. More details can be found here:
Personal data processed by students

14 – Automated Decision-Making

Profiling
Profiling is the automated analysis of aspects of an individual's personality, behaviour, interests and habits to make predictions or decisions about them.

Automated decision-making
Automated decision-making is the process of making a decision by automated means without any human involvement.

Data subject rights
Data subjects have the right to object to automated decision-making and profiling on grounds relating to their particular situation. The University is specifically required to provide for this right in all cases where processing is based on the legal bases of 'public task' and 'legitimate interest'.

Once the data subject exercises this right, the University must interrupt (or avoid starting) the profiling or decision-making process unless it can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject. The University may also have to erase the relevant personal data.

The prohibition

There is a clear prohibition regarding decisions based solely on automated decision making and/or on profiling, but only if they produce legal effects or which similarly significantly affect an individual.

"Legal effects" have an impact on a data subject's legal rights, affect a data subject's legal status or their rights under a contract. An example would be marking exam essays using solely AI leading to students failing their exams.

"Similarly significantly affects" means the processing must be more than trivial and must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly influence the circumstances, behaviour or choices of the data subjects concerned. An example would be deciding on applications to study solely through AI.

There are three exceptions from that prohibition, and that is where automated decision-making:

- is necessary for the performance of or entering into a contract;
- is authorised by law; or
- is based on the data subject's explicit consent

Even where the three exceptions apply and automated decision-making and profiling can be used, data subjects still have rights. They can still object to the automated processing and request that a human being become involved and reconsider the decision.

If you believe that you are using automated processing or profiling, contact the DPO at dpo@ed.ac.uk.

Specific examples

Exam marking: The University does not use solely automated decision-making when marking exams. Even multiple-choice tests that may be checked and marked by automated means do not fall under the definition of solely automated decision-making, as the exam has been set by a human being, the correct answer has been determined by a human being and the automation applies only to checking the given answers against the correct one.

Learning analytics: When using learning analytics, the University will take the following approach as regards the legal basis:

- Use legitimate interests as the legal basis for the processing of non-sensitive personal data for analytics
- Obtain consent for processing of special category data
- Obtain consent to make interventions directly with students on the basis of the analytics.

In accordance with the rights set out above under section 11, individuals can object to the processing where legitimate interest is the legal basis. For the situations where consent is required, that consent can either be withheld or withdrawn at any time.

15 – Data Protection by Design and Default

Data protection by design (also called 'privacy by design') is an approach to projects and initiatives involving personal data that is intended to incorporate data protection compliance from the start, rather than considering it as an after-thought.

Thus, the University is required to implement the appropriate technical and organisational measures both at the time when the methods and ways of processing personal data are determined and also at the time of the processing itself. In addition, the University will need to ensure that, *by default*, only personal data that are necessary for each specific purpose are actually processed.

Examples for technical and organisational measures are:

- Data minimisation
- Additional layers of encryption
- Data retention limits
- Restricted access
- Anonymization and pseudonymisation
- Encryption, hashing, salting

All staff and agents of the University are required to apply the data protection by design principles when developing a new project or reviewing existing projects that involves the use or storage of personal data. The guidelines below explain the types of project or initiative when this might be relevant, what data protection by design is and what measures can be put in please to protect personal data.

Data Protection Impact Assessments: One important measure that is expressly listed in the UK GDPR as a mandatory requirement is conducting a Data Protection Impact Assessment (DPIA) for projects or initiatives that may have a negative impact on data subjects' privacy. A DPIA is a type of risk assessment whereby potential privacy issues and risks are identified and examined from the perspective of all stakeholders.

A DPIA should be done as part of the initial phase of a project to ensure that risks are identified and taken into account before the problems become embedded in the design and causes higher costs due to making changes at a later stage. Also, if there is a change to the risk of processing for an existing project a review should be carried out.

The DPIA will then continue to assess privacy impacts throughout the lifespan of the project. Examples of the types of projects where a DPIA needs to be considered include:

- Building or buying new software or IT systems for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A new surveillance system such as CCTV
- Using personal data for new purposes such as a new database which consolidates information held by separate unrelated parts of the University.

In addition to meeting legal requirements, taking a proactive approach to privacy will reduce the likelihood of fines or financial losses due to data protection breaches and help build reputation and stakeholder confidence.
Guidance on how to conduct a DPIA can be found here:
Data Protection Impact Assessment and Guidance

Pseudonymisation: Pseudonymisation is a privacy-enhancing technique; it is a process rendering data neither completely anonymous nor directly identifying. With pseudonymisation you separate personal data from direct identifiers so that linkage to an identity is no longer possible without the additional information that is held separately. It is important to note that pseudonymised data is not exempt from the UK GDPR and the DPA, it is still considered personal data.

If you pseudonymise a research dataset by keeping the data and the identifiers separate and send the pseudonymised data to another University without also sending the identifiers, then the other University will process anonymised data as the UK applies a concept of relative anonymity. You, however, will still process personal data as you can still at any time re-identify individuals. In countries such as Belgium, the other University would still process personal data as the key exists somewhere in the world – Belgium applies a concept of absolute anonymity.

Under certain circumstances, pseudonymised data can be exempt from data subject rights. This exemption, however, applies only if you are able to demonstrate that you are not in a position to identify the data subject anymore, e.g. when you destroy the identifiers but you know that they still exist elsewhere. You will then not be required to comply with subject access requests, as the UK GDPR does not require a controller to hold additional information for the sole purpose of complying with such requests. If, however, data subjects provide you with the additional information you would require to re-identify them in the data set, they must be permitted to exercise their rights.

Anonymisation: Anonymised data means that all identifiers have been irreversibly removed from data subjects and they are no longer identifiable in any way. In this case, the UK GDPR and the DPA do not apply any longer – the data is no longer personal. However, with the advances in modern technology, re-identification will become easier. The ICO uses applies the concept of the ‘motivated intruder’: data will be considered anonymous unless an individual has the motivation to spend a considerable amount of time, effort and/or resources to re-identify people.

16 – Direct Marketing

Direct marketing includes the advertising or marketing of commercial products or service, as well as fundraising, and includes all messages promoting an organisation, such as promoting University events or opportunities for students.

Direct marketing covers all forms of communication, such as marketing by letter, telephone, email and other forms of electronic messages.

Finding the correct legal basis for direct marketing is very important. The law distinguishes between direct marketing using electronic means and non-electronic means. Currently, 'electronic means' covers the use of email and text messaging.
For marketing by letter and telephone (unless the individual is registered with the Telephone Preference Service), the UK GDPR applies and your legal basis can be 'legitimate interest' – you will not need consent.

The Privacy and Electronic Communications Regulations 2003 (PECR) regulate the use of electronic communications such as email or text messaging as a form of marketing. Electronic marketing to private individuals can only be done with consent as the legal basis. Consent must be 'opt-in' and any direct marketing messages should only be sent to those people who have in fact opted in. One exception to the need to obtain prior consent is the so-called 'soft opt-in', which is based on 'legitimate interest'. Soft opt-in can be used in situations where you have a pre-existing commercial relationship with the individual, as long as you provide the option to 'opt out' (unsubscribe) in every email and inform people when you collect their data that there will be marketing and that they can opt out.
The full guidance on direct marketing can be found here:
Direct Marketing under Data Protection Law

17 – Data Protection Breaches

A data protection breach is defined in UK GDPR to mean:

> "a breach of security leading to the accidental or unlawful destruction, loss, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The UK GDPR imposes a requirement that certain data protection breaches are reported to the Information Commissioner's Office within 72 hours of the University becoming aware of the breach.

While the University makes every effort to avoid data protection breaches, it is possible that mistakes will occur on occasions or things will happen that are beyond the University's control. This section of the Handbook sets out the procedures to follow if a personal data incident has occurred. All individuals who access, use or manage the University's information are responsible for following these guidelines and for reporting any data protection incidents that come to their attention.

A personal data incident can occur for a number of reasons some examples of these include:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Unauthorised disclosure (e.g. email sent to incorrect recipient or document posted to the wrong address or personal information posted onto the website without consent)
- Human error;
- Unforeseen circumstances such as a fire or flood;

- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

Reporting an incident
It is the responsibility of any staff, student or other individual who discovers a personal data incident to report it **immediately** to the office of the DPO at **dpo@ed.ac.uk** with 'breach' in the subject line. You will then have to fill in a Breach Evaluation Form, which can be found here:
Breach Evaluation Form

The DPO will require information from you about the nature of the breach, i.e. what happened, and whether any personal data was involved. This could be the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

The DPO will determine whether the incident constitutes an actual data protection breach and will act accordingly to help you contain the incident and, where necessary, assist with notifying the affected data subjects. The DPO will also, where required, notify the Head of College, School or Department, the University Secretary and the Information Commissioner's Office.

The DPO will keep a record of all data protection incidents and breaches including the actions taken to mitigate the breach and the lessons learnt.

18 – Mailing lists

Privacy notices: Whether your communication is internal or external, electronic or in paper format, you must always ensure that recipients receive a privacy notice, through either a link or the entire privacy notice in the footer of all emails, and a link or the entire privacy notice included in all letters sent out.

External mailing lists in paper format: If your external mailing list is used to send communications in paper format, you will not need to obtain consent. Instead, your legal basis is 'legitimate interest'. You must, however, provide recipients with the opportunity to easily and effortlessly opt out of receiving the communication in every letter.

External mailing lists in electronic format:
Business-to-business (B2B)
If you send emails to business contacts, i.e. individuals who can be considered as representatives of their company, organisation or institution (e.g. students or academics from another university), you can rely on 'legitimate interest'. However, you must first provide a privacy notice and then the option to opt out in every communication.

Private individuals

If you send emails to private individuals, then you must have obtained consent. After an appropriate period of time, consent must be refreshed. Always provide first a privacy notice and then the option to opt out in every communication.

Mixed lists
If your mailing list contains both B2B contacts and private individuals and you have not obtained consent from the private individuals, conduct a risk assessment to determine whether continuing to send emails is likely to cause offence or distress or whether receiving the emails is in the individuals' interest and/or to their benefit.

Email service provider
The University uses dotdigital for email marketing lists. Guidance can be found here:
Dotdigital guidance

Internal mailing lists in electronic format: For essential business mailing lists with information such as changes in lecture theatre for students, information about lack of heating or power failure in certain buildings, subscription is mandatory and an option to unsubscribe cannot be given and the legal basis for these emails is 'contractual obligation'.

For non-essential mailing lists about, for example, events in a School or career opportunities for students, staff members and students are considered to be business contacts, and the legal basis for these emails is 'legitimate interest'. Always provide the option to opt out in every communication.

Mailing list service: For internal mailing lists using sympa, guidance can be found here:
Sympa guidance

The full guidance on mailing lists can be found here:
Mailing lists and data protection

19 – CCTV

For CCTV systems, two types must be distinguished:
- Cameras that record
- Cameras that only show live footage but don't record

Both types fall under the UK GDPR and the DPA as both process personal data through electronic means.

The legal basis for both types of CCTV depends on the purpose for the cameras, which can range from 'legal obligation' over 'public task', 'contractual obligation' to 'legitimate interest'.

Individuals whose images are recorded have a right to view the images of themselves and to be provided with a copy of the images.

Further guidance can be found in the CCTV policy:
CCTV Policy

20 – Photography

Whenever individuals can be identified by their image, data protection legislation applies. In these situations, the rights of the individuals for collection and use of their photographs must be respected – they must be informed when an identifiable image of them will be or has been captured, and a legal basis must be found before the image is used in any way.

Photographs of individuals and posed groups: When taking photographs of a specific person, you should use 'legitimate interest' as your legal basis.

If you intend to post the photographs on the internet, that constitutes international transfer and you will need a safeguard. This means that you will need to obtain written consent of the individuals to have their images posted online.

Photographs of crowds: If crowd shots are taken during an event and the individuals are not identifiable, then it is not necessary to have a legal basis to take, display or publish the photo. This applies to any individuals, students and staff whose images are incidental detail, such as in crowd scenes for graduation, conferences and in general campus scenes. If the photos are taken at a conference where it is likely that individuals may be identified even in crowd scenes, then your legal basis is 'legitimate interest'.

You must, however, include notices at the event informing attendees of the fact that photo are being taken so they have the opportunity to opt out.

Photographs of children: If taking photographs of children, you must obtain consent from a parent or guardian. This may be written or verbal depending on the circumstances, see the guidance above.

The full guidance on photography can be found here:
Photography guidance

Version number	Author/editor	Date	Edits made
4	DPO	January 2019	Updated
5	ADPO	August 2019	Links and minor text updated
6	DPO	January 2020	Minor changes to text. Adequacy countries updated.
7	DPO	June 2020	Links updated
11	DPO	July 2024	Major changes made