Privacy Notice Guidance

This guidance is intended to assist with the writing of simple/basic privacy notices. It is not intended to provide in-depth knowledge of the relationship between privacy notices, GDPR and PECR (Privacy and Electronic Communications Regulations). The ICO has a [comprehensive guide on writing privacy notices.](https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/)

**If you intend using any information gathered on your forms for marketing purposes (or will be passing to another department who will use data for these purposes) please contact** **gdpr@derby.ac.uk** **for guidance.**

**This guidance assumes the University of Derby is the Data Controller and no information is being passed to a third party for processing on our behalf. If this is not the case please contact** **gdpr@derby.ac.uk** **for guidance.**

**If you need any help, guidance or support please contact** **gdpr@derby.ac.uk**

ITS have provided 3 basic templates for privacy notices (templates below). They cover internal, external and small data capture forms. The templates have been created to comply with GDPR and ICO good practice. The notices can be adapted for your purposes by amending the highlighted sections in each of the templates. Before you complete the template, please ensure you have read and understood the guidance below.

# 1. Things to consider:

1. If you share the data, include uses and retention for those people you share with.
2. If there is a legal requirement for you to retain data, reference the associated law.
3. Be clear and concise and suitable for the intended audience (e.g. you may choose to use different wording for children than you would for adults)
4. You should not rely on consent. This should only be used if there is a reason to obtain the data and no other lawful reason applies (see section 2).

# 2. Lawful basis to process personal information

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual. You must be able to demonstrate that a lawful basis applies.

1. Consent: the individual has given clear consent for you to process their personal data for a specific purpose (see ‘Consent as a lawful basis’).
2. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
3. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
4. Vital interests: the processing is necessary to protect someone's life.
5. Public task: the processing is necessary for you to perform at task in the public interest or for your official functions, and the task or function has a clear basis in law.
6. Legitimate interests: the processing is necessary for your legitimate interests or the interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing due to perform your official tasks.)

Consent as a lawful basis:

* Consent requires affirmative action e.g. if using opt-in/out boxes the data subject must actively opt-in. Don't use pre-ticked boxes or any other method of default consent.
* Consent must be kept separate from other terms and conditions
* Be specific and granular, you must gain consent for separate things. Vague or blanket consent is not enough.
* It must be easy for people to withdraw their consent and details of how to do this must be included. The same mechanism used to give consent should be available to withdraw that consent e.g. if you gain consent via email, an email address to withdraw consent must be provided.
* You must keep evidence of consent e.g. when this was given, who gave it, how it was given.
* Consent must be genuine and provide the data subject with control over the use of their data. If consent is requested then it should be possible for consent to be withdrawn. For example, if consent was given to use data for statistical analysis and then the data subject withdrew their consent it must be possible for them to do so. If in reality you could not remove the data then you should not use consent as the lawful basis for processing. If there are any restrictions on withdrawal of consent this must be made clear.

# 3. Special Categories of Data

In addition to lawful basis, if you are collecting or processing special categories of data you must also identify a special category condition. Special categories are:

Race, Ethnic Origin, Politics, Religion, Trade Union Membership, Genetics, Biometrics, Health, Sex Life, Sexual Orientation.

GDPR (article 9) states "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation **shall be prohibited."** Exceptions to this are detailed below.

**Special Category Conditions:**

1. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to above may not be lifted by the data subject;
2. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
4. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
5. processing relates to personal data which are manifestly made public by the data subject;
6. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
7. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
8. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
9. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
10. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4. Privacy Notices and Marketing

In addition to GDPR additional legislation (PECR – Privacy and Communications Regulations) applies to electronic marketing. The templates within this document are not appropriate for marketing use, please contact GDPR@derby.ac.uk for additional guidance and support.

# 5. How to complete a Privacy Notice template

* Ensure you have read and understood the guidance above.
* If the University is not the data controller or the data collected will result in marketing activity DO NOT USE the templates. Contact gdpr@derby.ac.uk for advice.
* Select the correct template.
* Copy and paste the text into your document.
* Under each template heading you are provided with a colour coded letter, this directly corresponds with the colour coded letter within the privacy notice template. Amend the information in each notice following the instructions.
* If you need any help contact gdpr@derby.ac.uk

## Template 1 – For Internal Forms and Data Collection Activities

## Instructions:

**A** – amend to identify the data collection method (e.g. webform, form etc.)

**B** – detail what the information supplied will be used for.

**C** – if applicable include the text: and in line with Health and Safety

**D** – if there is a need to contact the data subject include an explanation. If this is not required, delete 'We may contact you to'

**E** – Detail in years/months/weeks etc. how long data will be retained for. If there is a legal/statutory requirement state the act that applies.

**F** – amend with details of who information will be shared with. If data is not shared externally delete sentence

**G** – provide details of the lawful basis for processing and special category conditions if applicable

**H** – Only include if consent is the legal basis in which data is being processed. Data subjects should be able to withdraw their consent. If there would be a specific point where this would not be possible this would need to be identified. If consent is not required remove "I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk"

##

## Privacy Notice:

The information that you supply on this **A** will be held and processed in line with the Data Protection Act 2018 and GDPR.

Information will be used by the UoD (as Data Controller) to **B  C**

**D** We may contact you to

We retain this data for **E**, after such time it will be securely destroyed.

It will be shared externally with **F**

Our lawful basis for processing this data is **G**.

**H** I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk.

The DPO for the University can be contacted via GDPR@derby.ac.uk Further information on how we handle your information and details of our DPO can be found on our webpage <https://www.derby.ac.uk/its/datagov/privnotice/>

## Template 2 – Small Data Capture Cards (e.g. A5)

Instructions**:**

**A** – delete card/form as appropriate

**B** – detail what the information supplied will be used for.

**C** – if applicable include the text: and in line with Health and Safety

**D** – if there is a need to contact the data subject include an explanation. If this is not required, delete 'We may contact you to'

**E** – Detail in years/months/weeks etc. how long data will be retained for. If there is a legal/statutory requirement state the act that applies.

**F** – amend with details of who information will be shared with. If data is not shared externally delete sentence

**G** – provide details of the lawful basis for processing and special category conditions if applicable

**H** – Only include if consent is the legal basis in which data is being processed. Data subjects should be able to withdraw their consent. If there would be a specific point where this would not be possible this would need to be identified. If consent is not required remove "I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk"

## Privacy Notice:

The information that you supply on this **A** card/form will be held and processed in line with the Data Protection Act 2018 and GDPR.

Information will be used by the UoD (as Data Controller) to **B  C**

**D** We may contact you to

We retain this data for **E**, after such time it will be securely destroyed.

It will be shared externally with **F**

Our lawful basis for processing this data is **G**.

**H** I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk.

Our Data Protection Officer (DPO) is James Eaglesfield on (01332) 591762. Our Deputy DPO is Helen Rishworth on (01332) 591954. Alternatively you can email gdpr@derby.ac.uk Further information on how we handle your information and details of our DPO can be found here on our website <https://www.derby.ac.uk/its/datagov/privnotice/>

## Template 3 – For External or Student related data collection/processing activity.

## Instructions:

**A** – amend to identify the data collection method (e.g. webform, form etc.)

**B** – detail what the information supplied will be used for.

**C** – if applicable include the text: and in line with Health and Safety

**D** – if there is a need to contact the data subject include an explanation. If this is not required, delete 'We may contact you to'

**E** – Detail in years/months/weeks etc. how long data will be retained for. If there is a legal/statutory requirement state the act that applies.

**F** – amend with details of who information will be shared with. If data is not shared externally delete sentence

**G** – provide details of the lawful basis for processing and special category conditions if applicable

**H** – Only include if consent is the legal basis in which data is being processed. Data subjects should be able to withdraw their consent. If there would be a specific point where this would not be possible this would need to be identified. If consent is not required remove "I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk

## Privacy Notice:

The information that you supply on this **A** will be held and processed in line with the Data Protection Act 2018 and GDPR.

Information will be used by the UoD (as Data Controller) to **B  C**

**D** We may contact you to

We retain this data for **E**, after such time it will be securely destroyed.

It will be shared externally with **F**

Our lawful basis for processing this data is **G**.

**H** I give my explicit consent for my details to be used as stipulated Yes   No

As a data subject you can request withdrawal of consent at any time by contacting gdpr@derby.ac.uk.

Our Data Protection Officer (DPO) is James Eaglesfield on (01332) 591762. Our Deputy DPO is Helen Rishworth on (01332) 591954. Alternatively you can email gdpr@derby.ac.uk
Further information on how we handle your information can be found here on our website - <https://www.derby.ac.uk/its/datagov/privnotice/>