THE UNIVERSITY *of* EDINBURGH

GDPR IMPLEMENTATION CHECKLIST

UNIVERSITY OF EDINBURGH

TOOLKIT TO HELP UNIVERSITY BUSINESS UNITS COMPLY WITH THE NEW DATA PROTECTION LEGISLATION (GDPR)

This toolkit is issued by the University's GDPR Steering Group and provides a checklist of actions for University Business Units (such as College Offices, Schools, Administrative and Support Areas) to take to implement the changes necessary to comply with new legislation (the General Data Protection Regulation, GDPR and the Data Protection Act 2018, the DPA).

NOTE: This toolkit should be used in conjunction with the Data Protection Handbook and the University Retention Schedules to ensure that personal data is not retained longer than required.

CONTENTS

CHECKLIST OF ACTIONS

Section 1 – Data Processing Registers

CCBS note: Our data processing register is maintained by the Deanery of Clinical Sciences. All 'usual' UoE business is already covered in the register.

Ref	Action	Rationale	Complete [Y or N/A]
1.1	Ensure that your Business Unit's Data Processing Register contains details of the personal data that your Unit collects or processes. Schools should use the School Template as their basis and add to/delete from this Template accordingly.	Under the GDPR Data Controllers must demonstrate compliance. UoE's Data Protection Policy requires that Business Units must hold and maintain a record of all processing activities to evidence compliance with the legislation. CSE Data Processing Registers are available from: https://uoe.sharepoint.com/sites/CSCE/compliance/DataProtection/SitePages/Home.aspx	
1.2	Ensure that the Legal Basis for Processing and Retention Period, as outlined in the relevant Privacy Notice is updated within your Data Processing Register (refer 2.1).	The Registers need to record the Legal Basis for Processing and Retention Period for the data. While there was some initial assessment of these aspects, Business Units should be aligning these with what data subjects are advised in the relevant Privacy Notice	
1.3	Ensure that your Data Processing Register outlines the Privacy Notice that covers the processing that you undertake.	Refer 2.1. Recording this within the Data Processing Register will ensure any future changes in processing can be reflected in the relevant Privacy Notice, and provide a mechanism for ensuring all processing is covered.	

Section 2 - University privacy notices

Ref	Action	Rationale	Complete [Y or N/A]
2.1	Check that the University's privacy notices supplied to the following groups of people accurately reflect what you do with their personal information as outlined on your Data Processing Register. • Student Related: a) Student application privacy notice: https://www.ed.ac.uk/studying/admissions/privacy-statement b) Student privacy notice: https://www.ed.ac.uk/files/atoms/files/university_of_edinburgh__privacy_statement.docx c) Special Circumstances privacy notice: : https://www.ed.ac.uk/academic-services/students/privacy-notices • Alumni, Supporter and Donor Related: d) https://www.ed.ac.uk/development-alumni/privacy In addition, a short privacy statement highlighting key information must be provided to these individuals that includes a link to the full privacy notice. • Staff Related: e) Job applicant privacy notice: https://www.ed.ac.uk/human-resources/jobs/applying/applicant-privacy-notice	Under the GDPR we need to supply individuals with detailed statements (known as 'privacy notices') outlining how we will use their personal information. The University's core privacy notices are comprehensive and ensure that all of the necessary topics are covered. Business units must not use information in other ways that individuals don't know about. If these University privacy notices reflect what you do with their personal information, you do not need to provide your own, or a link to, the University privacy notice. If there are other uses, a customised privacy notice may need to be agreed with the Data Protection Officer – refer guidelines available on the Records Management GDPR website. Some template privacy notices, already approved by the Data Protection Officer, are there. Staff wishing to communicate with alumni should contact Development and Alumni at alumni@ed.ac.uk in the first instance to discuss their requirements.	

	f) Staff privacy notice: https://www.ed.ac.uk/human-resources/privacy-information-notice If you use personal information in other ways, consult the Data Protection Officer, or refer to sample privacy notices provided on the website		
2.3	If you currently inform any of the above groups of people about how their personal information is/will be used, ensure that your statements either are deleted or are replaced by a link to the core privacy notices.	It is not considered likely that many Business Units will supply 'local' privacy notices to these groups (except, e.g., where Business Units are directly responsible for admissions). In general, such 'local' privacy notices will be duplicative and can be deleted. Where they are needed, 'local' privacy notices should supplement – and not conflict with – the University's core privacy notices.	

Section 3 - Student applicants and students

Ref	Action	Rationale	Complete [Y or N/A]
3.1	Ensure that booking forms for student outreach/recruitment activities that you run contain links to https://www.ed.ac.uk/student-recruitment/about/use-of-personal-data	See Section 1.1. These standard privacy notices for outreach/recruitment events are comprehensive and ensure that all of the necessary topics are covered.	
3.2	If you run any online-only services (e.g. learning portals) used by children under 13 which collect their personal information (e.g. their contact details), implement a mechanism to collect consent from the children's parents. If you do outreach work in schools and collect/use children's personal data, and the children are younger than 12, ensure that the teachers have parental consent	Under the GDPR, children's use of 'information society services' requires parental consent if the child is under 13. (This age threshold will be set by the UK's Data Protection Bill – see Annex 1 – and so theoretically is subject to amendment.) Under Scots law, children from 12 onwards can consent to the use of their personal data.	

	Suggested wording is given in Annex 2.		
3.3	If you use students' personal information on the basis of those students' consent, check that you really need consent. If you do, ensure the consent is a genuine free choice and is recorded. *Suggested wording is given in Annex 2.*	Consent is one of the GDPR's 'legal bases' for processing personal data about individuals. It must be freely given, specific, informed, demonstrable and revocable. Nearly all of the University's uses of students' personal information should *not* rely upon consent. Consent forms and mechanisms should only be used when the individual has a genuine free choice as to whether they are happy for their personal information to be used in a particular way. Consents are not suitable for any core processes (e.g. exam marking) that have to occur regardless of a student's wishes, but they may be suitable in relation to purely subsidiary/supplementary activities (e.g. passing a cohort's names and contact details to a prospective employer)	
3.4	Ensure that your examination data retention policy is in line with the University's Student Records Retention Schedule, published at - https://www.ed.ac.uk/files/atoms/files//studentrecordsretentionschedulev15web.pdf	A central principle of data protection legislation is that personal data must not be kept for longer than necessary. The GDPR further requires us (in privacy notices) to tell individuals about data retention periods. These are standard retention periods for these sorts of records.	
3.5	Ensure that you have procedures in place to: (a) Delete or anonymise copies of unsuccessful student applications that may be held within your Business Unit in accordance with the retention times set in the privacy notice. (b) Delete or anonymise the non-EUCLID records of former students in accordance with the retention times set in your privacy notice, after their graduation/departure	A central principle of data protection legislation is that personal data must not be kept for longer than necessary. The GDPR further requires us (in privacy notices) to tell individuals about data retention periods. These are standard retention periods for these sorts of records.	

	(unless you require them solely for research/statistical purposes).		
3.6	Review your conversion communication to ensure the content is informative and does not contain marketing	There is a fine line between providing applicants with sufficient information to make an informed choice, and outright marketing. The guidance on marketing and GDPR will provide assistance to make this distinction.	

Section 4 - Alumni, current and potential supporters and donors

Ref	Action	Rationale	Complete [Y or N/A]
4.1	If you run any processes (e.g. webpages or forms) that ask University alumni to update their contact details, ensure that alumni are pointed to https://www.ed.ac.uk/alumni/services/portal	A central principle of data protection legislation is to keep personal data accurate. The use of Development and Alumni's update portal ensures that the University's central record, or 'golden copy', is accurate. https://www.ed.ac.uk/alumni/services/portal.	
4.2	If you manage any University hard copy or online donation forms, you must liaise with Development and Alumni to ensure the appropriate and legally required wording is included. Development and Alumni manage all philanthropic activity on behalf of the University and so you must consult with them prior to embarking on any fundraising related activity https://www.ed.ac.uk/development-alumni/staff	While this is not directly related to GDPR, it has been included in this document for the sake of completeness, as there are other regulations that must be considered when undertaking philanthropic activity.	
4.3	If you have a requirement to communicate with alumni/supporters/donors for any purpose, by post or electronically, make contact with Development and Alumni to ensure that the University holds an appropriate consent for each recipient and the appropriate opt outs or preferences, as requested by the individual, are applied. You can contact	While consent is not required under the GDPR either to hold personal information about alumni/supporters/donors or to contact them by post or phone (unless they are registered with the Telephone Preference Service), it is required in order to send them unsolicited electronic direct marketing (e.g.	

	alumni@ed.ac.uk to discuss your plans in the first instance or complete the online data request form https://www.ed.ac.uk/development-alumni/staff	fundraising) type communications (widely defined under the Privacy and Electronic Communications Regulations 2003, as amended). Development and Alumni holds a record of consents, opt outs and preferences obtained from alumni/supporters/donors and these apply University-wide.	
4.4	If you collect personal information from members of the public directly or indirectly (e.g. individuals booking to attend your events or sign up for news about your research or school or potential supporters/prospects interested in supporting the University), review and revise the information you supply to them at the point you collect their data. *Suggested wording is given in Annex 2 or link to the School Privacy Notice*	See Section 1.1. The University does not have a core privacy notice for members of the public, except for Development and Alumni activities (ref 2.1d); the uses made of their personal information will vary widely and so the information must be supplied by the individual Institution/project. The suggested wording in Annex 2 ensures that all of the necessary topics are covered. Alternatively, some Schools have adopted School Privacy Notices, which can be linked to. Full guidance on newsletters and mailing lists is available from the Records Management GDPR website.	
4.5	If you send newsletters, review and revise the privacy notice you provide when sending newsletters – ref 4.3 if you wish to communicate with alumni/supporters/donors. *Suggested wording is given in Annex 2 or link to the School Privacy Notice.*	Full guidance on newsletters and mailing lists is available from the Records Management GDPR website. Development and Alumni have developed this guidance specifically to help when communicating with alumni https://uoe.sharepoint.com/:b:/s/DACommunications/EeyS81OWAdtOj4ae5urFzQcBmI2wTbR9zYV7pL0oXW-D7w?e=0R6kc1	
4.6	If you send emails to members of the public that class as electronic direct marketing, ensure that you have collected and recorded their consent to do this – ref 4.3 if you wish to communicate with alumni/supporters/donors.	See Section 3.3. The suggested wording in Annex 2 ensures that consents are collected appropriately.	

	Suggested wording is given in Annex 2.	Development and Alumni have developed this guidance specifically to help when communicating with alumni https://uoe.sharepoint.com/:b:/s/DACommunications/EeyS81OWAdtOj4ae5urFzQcBmI2wTbR9zYV7pL0oXW-D7w?e=0R6kc1	
4.7	If you take room bookings, review and revise the privacy notice you provide when collecting any personal information. *Suggested wording is given in Annex 2.*	See Section 1.1.	
4.8	If you publish alumni/supporter/donor profiles or photos on a publicly available website, ensure you have their consent to do so. Full guidance on photographs is available from Records Management GDPR website.	The publication of photographs on a public website must be via consent.	

Section 5 - Job applicants and staff

Ref	Action	Rationale	Complete [Y or N/A]
5.1	Ensure that you follow standard University procedures (and use standard wording) when procuring references for job applicants (as outlined at https://www.edweb.ed.ac.uk/human-resources/recruitment/recruiters-guide/appointment/pre-employment-checks	The reference request template contained within the University procedures ensure that referees are adequately informed of the right of the applicant to see a copy of their references upon request, which is a central right of data protection legislation.	
5.2	Ensure that you follow standard University procedures when engaging temporary workers (as outlined in the University's Hiring Agency Workers Policy at https://www.ed.ac.uk/human-resources/recruitment/recruitment-policies)	These procedures ensure that temporary workers are adequately informed of their confidentiality and data protection obligations (in ways that mirror staff employment contracts).	
5.3	Review your Unit's policy and procedure in relation to hosting academic visitors and honorary staff, to ensure they are	Business Units have responsibility for approving and managing visitors, and are therefore responsible for ensuring visitors are made aware that they must	

	adequately informed of their confidentiality and data protection obligations.	comply with the University's confidentiality and data protection obligations.	
5.3	Ensure that you have procedures in place to: (a) Delete or anonymise copies of unsuccessful job applications in accordance with the retention times set in the Privacy Notice after the completion of the relevant recruitment exercise. (b) Delete or anonymise the non-HR Oracle records of former staff in accordance with the retention times set in the Privacy Notice after their departure (unless you require them solely for research/statistical purposes). (c) Delete emails and other records related to staff once the information has been entered in the relevant HR system.	See Section 2.5.	

Section 6 - Research

Ref	Action	Rationale	Complete [Y or N/A]
6.1	Ensure that your academic and research staff (especially Principal Investigators) are aware of the guidance on research involving personal data published on the Records Management GDPR website	The GDPR applies to personal data processed for academic and research purposes but there are significant exemptions from the standard provisions when processing personal data for research/statistical purposes. (The UK's Data Protection Act 2018 – see Annex 1 – contains many of these exemptions.) Academic researchers will need to read the guidance to determine which aspects of the GDPR apply to their research and which do not, and then will need to ensure that relevant provisions are followed. It should be stressed that many types of academic research will also be subject to ethical or regulatory	

		expectations (such as the need to seek informed consent from participants, even where not required by law) in addition to GDPR requirements. These will be explained in the guidance.	
6.2	Ensure that your academic and research staff (especially Principal Investigators) are: a) Aware of the guidance on research data management accessible from https://www.ed.ac.uk/records-management/training/research-data-management b) Complete the researcher data protection training course accessible from LEARN. c) Aware of the legal obligation to conduct a DPIA.	The GDPR heightens the importance of good information handling, including appropriate research data management techniques. Researchers need to be aware of best practice measures for personal data collection, handling, security and sharing (including the appropriate deployment of anonymisation and related techniques). All research projects also need to undergo a Data Protection Impact Assessment (i.e. a documented assessment of how the project can be conducted so as to minimise the privacy risk to the participants), especially where the project involves sensitive information such as the health or ethnicity of the participants. For most research projects, this DPIA will be included in the ethics approval form, however, some funders or data providers may insist on an external, separate DPIA.	

Section 7 - Institutional management

Ref	Action	Rationale	Complete [Y or N/A]

7.1	If you have issued a Business Unit specific Data Protection Policy or Statement, review it against the University Data Protection Policy to determine whether your local policy is still required. If you determine that it is, revise it as necessary to ensure that it is consistent with the University policy. *Business Units will be advised as soon as the University policy is available.*	Under the GDPR we need to demonstrate that we are following the law, and the appropriate deployment of data protection policies is one aspect of this. The University currently has published an updated Data Protection Policy on 25 May 2018 .	
7.2	If you have designated a particular member of staff as your Data Protection Officer, change their role title to Data Protection Champion.	The role and statutory functions of a Data Protection Officer (DPO) are explicitly set out in the GDPR. The University as a whole can only have one DPO and, while the concept of departmental data protection representatives/champions is beneficial, those individuals cannot formally be designated as DPOs.	
7.3	Appoint at least one member of staff as your Data Protection Champion. [CCBS note: Rebecca Devon is the CCBS Data Protection Champion]	Heads of Schools and Colleges and Managers of Administrative and Support Services have a responsibility to ensure compliance with the GDPR, the DPA and the University's Data Protection policy, and to develop and encourage good information handling practices within their areas of responsibility. Every College, School and Department must nominate one or more Data Protection Champion. These individuals are the first point of contact for data protection questions in their area, escalate difficult questions to the Data Protection Officer and act as a channel of communication between the Data Protection Officer and their area. Heads of Schools may choose to delegate the management of, but not the responsibility for, data protection matters within their business unit. The list of University Data Protection Champions is available from: https://www.wiki.ed.ac.uk/display/FoIP/Data+Protection+Champions	

7.4	Ensure that your staff: a) Understand the fundamentals of data protection legislation, and especially the GDPR, by making them aware of https://www.ed.ac.uk/records-management/gdpr (and linked pages). b) Complete the online University data protection training course accessible via https://www.ed.ac.uk/records-management/training/data-protection. c) Complete the online Information Security training course accessible via https://www.ed.ac.uk/infosec/learning-about-protection/register-information-security-essentials d) Ensure that researchers **also** complete the researcher data protection training course (also referred to at 6 above).	Under the GDPR we need to demonstrate that we are following the law, and appropriate awareness-raising and training is one aspect of this.	
7.5	If you run any CCTV systems (as opposed to hosting those run by the University Security Office), ensure: a) That you have adequate signage to indicate that cameras are being used. b) That you have a procedure for the deletion or overwriting of older images. c) That you carefully control access to, and use of, the images.	CCTV images of identifiable people constitute their personal data. As a result, they must be adequately informed of the data collection through signage and other notices. In line with the data protection principles, the images should not be kept for longer than necessary and should be accessed appropriately and stored securely.	

	Suggested signage wording is given in Annex 2.		
7.6	Check that your records management and retention procedures are aligned with the retention periods advised to Data Subjects in the relevant privacy notice, and data is kept secure	The principle of not retaining personal data for longer than necessary (unless the personal data are being retained solely for archival or research purposes) has not changed from the DPA to the GDPR, but the guidance requires updating and refreshing.	
7.7	Review your contracts with data processors. Arrangements with University-approved IT suppliers or major technology companies (e.g. Amazon Web Services, Apple, Microsoft, Google, Eventbrite, Bristol Online Surveys, Dotmailer) are managed centrally. But if you contract out other services that involve the processing of personal data (e.g. cloud storage, online survey tools, web-based forms): *a)* Inform the Legal Services Office of those arrangements so they can review existing contractual arrangements and develop contract amendments if necessary b) Ensure that any contractual arrangements with your data processors comply with the GDPR, in particular with regard to: (is) the general data protection obligations of the data procesor; and (ii) the further data protection obligations of the data processor if they are based outside the EEA. c) Record this release of data outside the University against the relevant data category record within your Data Processing Register. *Advice on reviewing supplier contractual arrangements is given in Annex 2, however Legal Services will advise on this.*	Under the old DPA there has always been a requirement for the University as a 'data controller' to ensure that its data processors commit contractually to strong levels of information security. Under the GDPR these contractual obligations have been enhanced and need to be set out in greater detail. The GDPR also updates (but does not substantively alter) the old DPA's requirements regarding transfers of personal data outside the EEA, and methods of ensuring that personal data are kept safe when this happens.	

Section 8 - Institutional Systems and IT

Ref	Action	Rationale	Complete [Y or N/A]
8.1	**Publication of Staff/Student Contact Details/Photos on Intranet** If you publish student and/or staff profiles (including photos, contact details and room location) on an intranet or a wiki with restricted access, ensure that the individuals are made aware of this and provided with the opportunity to object. Suggested wording is given in Annex 2.	The publication of this information on a wiki is covered by the legal basis 'necessary for a legitimate interest' as this information (including photos) is required for the effective operations of university business. Individuals can object to this if they have a legitimate reason why their information and photograph should not be published. This is not an 'opt-out' option, but a legitimate reason must be provided and does not need to be accepted.	
8.2	**Publication of Staff/Student Contact Details/Photos on Publicly Available Website** If you publish student and/or staff profiles (excluding photos) on a publicly available website (not an intranet), ensure that the individuals are made aware of this and provided with the opportunity to object. *Suggested wording is given in Annex 2.* If you publish student and/or staff photos on a publicly available website, ensure you have their consent to do so. Full guidance on photographs is available from Records Management GDPR website.	The publication of profiles and contact details on a public website is covered by the legal basis 'necessary for a legitimate interest' as this information (including photos) is required for the effective operations of university business. Individuals can object to this if they have a legitimate reason why their information and photograph should not be published. This is not an 'opt-out' option, but a legitimate reason must be provided and does not need to be accepted. The publication of photographs on a public website must be via consent. .	
8.2	Review and update your website privacy policy or policies (i.e. statements describing how the website will use any personal information it collects) in line with University's guidance on the Website Support Wiki - https://edin.ac/uwp-gdpr-advice	See Section 1.1. These privacy notice obligations apply equally in relation to website users. Following the guidance will ensure that all of the necessary topics are covered.	

	Review website(s) which you manage in relation to personal data collected; and update the website privacy notice and cookie consent mechanism accordingly.		
8.3	Ensure that your staff understand information security requirements by making them aware of the resources and training modules at https://www.ed.ac.uk/infosec/learning-about-protection Staff were advised by Information Services Group of this mandatory training earlier this year.	Under the GDPR the organisational requirement to manage personal data securely, so as to ensure its confidentiality, integrity and availability, is set out more prescriptively than under the old DPA but in essence the GDPR reflects common standards of information security practice. Where changes are required they can usually be implemented at a technical level, but some involve awareness-raising to prevent human error leading to a security incident that results in a personal data breach.	
8.4	Ensure that your staff who design, build or procure new IT systems are aware of the need to include data protection considerations at an early stage of the planning process through completion of a Data Protection Impact Assessment (DPIA). Guidance is available from: https://www.ed.ac.uk/records-management/gdpr	Under the GDPR there is a requirement to embed data protection considerations 'by design' when commencing work on a new system or project, and in certain circumstances a Data Protection Impact Assessment (i.e. a documented assessment of how the work can be conducted so as to minimise the privacy risk to the individuals) might be required. This requirement is being integrated into standard IT procurement processes but the same principles should be applied to IT systems built or amended in-house.	

ANNEX 1 - KEY FACTS ABOUT THE GDPR AND THE UNIVERSITY'S PREPARATIONS

Key facts about the GDPR

1. The General Data Protection Regulation (GDPR) came into force in the UK and the rest of the EU on 25 May 2018 and replaced the Data Protection Act 1998 (DPA). The GDPR is designed to harmonise and strengthen data protection law and practice across the EU. Like the old DPA, it is regulated and enforced in the UK by the Information Commissioner's Office (ICO). It will apply in the UK despite (and beyond) Brexit. It is supplemented in the UK by the Data Protection Act 2018 that was introduced in Parliament in September 2017 and became law by May on the same day as the GDPR. Amongst other things, the new DPA legislates in those areas where the GDPR gives EU Member States the discretion to vary the rules, and it sets out the ICO's regulatory powers in more detail.

2. Like the old DPA, the GDPR sets out rules and standards for the use of information about living identifiable individuals and applies to all organisations in all sectors, both public and private. It doesn't apply to anonymous information or to information about the deceased. The GDPR's rules and standards are based around the existing DPA concepts of data protection principles and individual rights. Accordingly, many of the concepts in the GDPR and reflected in this document are updated from current provisions in the DPA; others are new but they will become more familiar as the new law becomes embedded within all organisations.

3. Under the GDPR, the data protection **principles** state that personal data shall be:
   - Processed (i.e. collected, handled, stored, disclosed and destroyed) fairly, lawfully and transparently. As part of this, an organisation must have a 'legal basis' for processing an individual's personal data (e.g. they have consented to the processing, or the processing is necessary to operate a contract with them, or the processing is necessary to fulfil a legal obligation).
   - Processed only for specified, explicit and legitimate purposes.
   - Adequate, relevant and limited.
   - Accurate (and rectified if inaccurate).
   - Not kept for longer than necessary.
   - Processed securely.

4. Under the GDPR, an individual's **rights** (all of which are qualified in different ways) are as follows:
   - The right to be informed of how their personal data are being used. This right is usually fulfilled by the provision of 'privacy notices' (also known as 'data protection statements' or, especially in the context of websites, 'privacy policies') which set out how an organisation plans to use an individual's personal data, who it will be shared with, ways to complain, and so on.
   - The right of access to their personal data.

- The right to have their inaccurate personal data rectified.
- The right to have their personal data erased (right to be forgotten).
- The right to restrict the processing of their personal data pending its verification or correction.
- The right to receive copies of their personal data in a machine-readable and commonly-used format (right to data portability).
- The right to object: to processing (including profiling) of their data that proceeds under particular legal bases; to direct marketing; and to processing of their data for research purposes where that research is not in the public interest.
- The right not to be subject to a decision based solely on automated decision-making using their personal data.

5. The GDPR is more prescriptive than the old DPA about how organisations need to implement the above broadly defined provisions and it also introduces a range of **accountability requirements** to encourage a proactive and documented approach to compliance. These accountability requirements include:
   - Implementing policies, procedures, processes and training to promote 'data protection by design and by default'.
   - Having appropriate contracts in place when outsourcing functions that involve the processing of personal data.
   - Maintaining records of the data processing that is carried out across the organisation.
   - Documenting and reporting personal data breaches.
   - Carrying out Data Protection Impact Assessment on all new processing activities.

6. The GDPR and the Data Protection Act 2018 also set out various exemptions from the principles, rights and accountability requirements when personal data are processed for certain purposes. The following are of particular note in an HE context:
   - Personal data processed for journalistic, artistic, literary or 'academic purposes' are exempt from the principles and almost all of the rights, though not the accountability requirements. For these exemptions to apply, publication must be envisaged *and* that publication must be in the public interest. These exemptions are particularly (though not exclusively) relevant for research studies in the humanities and social sciences that are akin to journalistic or commercial writing and where freedom of speech would be compromised by the application of the relevant parts of the GDPR (e.g. writing a biography of a living political figure).
   - Personal data processed for 'scientific or historical research purposes', 'statistical purposes' or 'archiving purposes in the public interest' are exempt from two of the principles (those stating that personal data shall be processed solely for specified purposes and not kept for longer than necessary) and most of the rights, though not the other principles, the right to be informed (unless providing the privacy notice would be impossible or would involve 'disproportionate effort'), or the accountability requirements. For these exemptions to apply the processing must not result in individual decision-making about the data subjects *and* the processing must not cause them substantial damage/distress *and* the publication of the research results must not identify any data subjects. These exemptions are particularly (though not exclusively) relevant for research studies in the social and biomedical sciences that involve human participants

(e.g. running an online sociological test that collects personal data from volunteers) or where personal data collected for other purposes are re-used (e.g. carrying out secondary analysis on clinical scans that are linked to individual patients).

Key facts about the University's preparations

7. The University has established a GDPR Steering Group to oversee the University's implementation of GDPR. This Committee is chaired by the University's Deputy Secretary of Strategic Planning and with representation from each of the three Colleges, ISG, University Secretary's Group and Corporate Services. The Steering Group receives advice from the University's Data Protection Officer, who also attends meetings.

8. Most changes required for the GDPR can be fulfilled by making subtle but important changes to major systems and central processes. Some of these concern the core interactions with, and privacy notices supplied to, different types of individual such as applicants, students, alumni and staff. Others relate to the overarching policies, procedures and records that are required to enable us to demonstrate our compliance with the new law.

9. Because Edinburgh is a devolved University, some changes are required at Business Unit level. This document is designed to guide Business Units in thinking about the changes they will need to make and how they might implement them.

10. More detailed guidance on GDPR will be available in a Data Protection Handbook, and from various guidance materials currently available on the University's Records Management website at: https://www.ed.ac.uk/records-management/guidance/data-protection

Further information

See https://www.ed.ac.uk/records-management/gdpr

ANNEX 2 - SUGGESTED TEMPLATE WORDINGS

These wordings are suggestions. Business Units should adopt the most suitable language for the situation and, most importantly, whatever is said should be factually accurate.

Note Ref	Brief description	Suggested wording
3.2	Wording for parental consent mechanism	If you are aged **under 13**, we will need consent from your parent or guardian in order to sign you up for [this service]. Please provide us with their email or postal address so that we can write to them to collect this. We will not be able to offer you [the service] until we receive consent from your parent or guardian.
3.3	Wording for student consent to specific data use Note that if you ask for consent for more than one aspect, you will need to list each aspect and provide students with the option to consent to each aspect separately, e.g. via tick boxes	Please [sign/electronically sign/tick], date and [return by XXX/return by email/submit] the below declaration: I consent to the [Business Unit name] using my personal data for [describe the specific purpose] and understand that I can withdraw my consent at any time.
4.4	Wording when collecting personal information from members of the public as part of event registration	*Note: This has been designed to be used for event registrations – conferences, workshops, etc. and should be amended to accurately reflect what data you collect, use etc. as well as how long you retain data.* **Information about you: how we use it and with whom we share it** We will use your personal data to allow us to process your registration, communicate with you and obtain your feedback about the event. We are processing the information about you for these purposes because by registering for the conference, you give your consent for us to do so. We will also contact you about future events you might be interested in if you have given your consent to this. You may opt out of this at any time. (We will also use your information to track …. because it is important for the University to know…/be able to follow up….. /measure the effectiveness of…. If you would prefer us not to do so, please email us at …..)

		In order to facilitate online bookings for our events, we use ……. - a third party service which is not operated by the University of Edinburgh. Details of ……. privacy policy can be found at: If you wish to attend an event organised by ……, but do not wish to use ……, please email us at: …. (insert email) If you have given us your permission, we will share your name, affiliation and contact details with the other participants in the delegate list. We will not share information about you with any other third party. We will hold the personal data you provided us for 6 months. If you have agreed to be contacted about future events, we will hold your personal data for as long as you subscribe to these updates. Financial data such as a payment record will be held for 7 years, but we will ensure that all information that can identify you directly is removed after 6 months. We do not use profiling or automated decision-making processes. If you have any questions, please contact… [insert role title and email address for local contact within school/department] This Privacy Statement is continued at: edin.ac/privacy
4.5	Wording when sending newsletters or collecting personal information for the purposes of a mailing list	*Note: This has been designed to be used for mailing lists for general communication, such as news and events.* **Information about you: how we use it and with whom we share it** [Name of Unit] processes the personal data of [our internal and external stakeholders or whoever has signed up to the mailing list], in order to [deliver and improve the opportunities and services we provide in a personalised manner or what the newsletter etc is about and what its used for], to ensure each individual receives relevant information and to ensure we use resources in the most efficient and effective way. To do so, we are using [Dotmailer] as our mailing system. The information you provide will be used by the University to: *[Amend following as necessary to reflect what you use this for]* • Keep you up to date with news and progress regarding the University

		• Provide you with information on any services you have requested and the promotion of benefits and services • Ensure we only communicate with you about events, opportunities, or services of interest to you We are currently using information about you because you have previously given us consent to be added to our newsletter mailing list. We will hold the personal data you provided us for 1 year. After this period we will send communication to you querying whether you wish to remain on our mailing list. Alternatively, you can opt out of the mailing list at any time. We do not use profiling or automated decision-making processes. A human decision maker will always be involved before any decision is reached in relation to you. If you have any questions, please contact: XXXX View the continuation of this privacy statement on the University of Edinburgh website edin.ac/privacy
4.6	Wording when collecting email marketing consents from members of the public	We'd like to keep in touch with you to [keep you informed about our activities/invite you to future events]. Please tick the boxes below to indicate the formats in which you are happy to be contacted (you can change these at any time by contacting [email address] or automatically unsubscribing to emails or texts): ☐ Email ☐ Text ☐ Phone
4.7	Wording when collecting personal information as part of room bookings	*Note: This has been designed to be inserted above the 'submit' button on a room-booking site or, if paper-based, on the form.* The University of Edinburgh <name of unit> will use this information under the legal basis of contractual necessity. The information collected in this form is used to provide you with information about specific facilities to meet your requirements, and will be stored on <eg. Salesforce, a piece of Customer Relationship Management software>. If you choose to proceed with a booking, we will share the information with other University of Edinburgh teams, such as invoicing, to ensure all operational aspects of the School's facilities meet your requirements. Your information will be retained for 5 years after the event has passed for statistical purposes. We do not forward this

		information to third parties and it's not used to contact you about additional events. If you choose to cancel your event room booking, you will not be contacted again. If you have any questions, please contact: XXXX View the continuation of this privacy statement on the University of Edinburgh website edin.ac/privacy
7.4	Wording for CCTV signage	The University of Edinburgh operates CCTV on these premises for the purposes of safety and security. For further information please phone [contact number].
7.5	Wording for publication of photograph on publicly available website	☐ I hereby consent to the University capturing my image in photography and/or video recordings. ☐ I hereby consent to the University using my image when I have been caught in photography and/or video recordings, taken/recorded on …… [insert date] at…… [insert location] for use in …… [insert details] ☐ I hereby consent to the photographs and/or video recordings being used in other University-wide marketing and promotional communications, including on the University website, in University social media, and on University hoardings. ☐ I hereby consent to the photographs and/or video recordings being used by University-associated third parties, on their websites or elsewhere in their marketing materials. I understand that: • my images will be held in accordance with the General Data Protection Regulation and the Data Protection Act 2018; • my image will be held indefinitely, for promotional purposes, unless I withdraw my consent; • I can withdraw my consent at any time by emailing [insert email address]. I understand that if the photograph has already been used in printed publications, then the University will not be able to recall all documents in which the image has appeared. However, the University will delete my image from their database and will go to all reasonable efforts to stop using the image in future. Signature: Print Name: Date: Address: