UNIVERSITY OF CAMBRIDGE
GDPR DATA PROTECTION WORKING GROUP

TOOLKIT TO HELP UNIVERSITY INSTITUTIONS PREPARE FOR NEW DATA PROTECTION LEGISLATION (GDPR)
NOVEMBER 2017

This toolkit is issued by the University's GDPR Data Protection Working Group. It provides a checklist of actions for University Institutions (i.e. any academic Faculty or Department within one of the six Schools, as well as relevant Non-School Institutions) to take to implement the changes necessary to comply with new legislation (the General Data Protection Regulation, GDPR). This legislation comes into force on 25 May 2018 and it replaces the Data Protection Act 1998 (DPA).

CONTENTS

CONTACT FOR QUESTIONS

James Knapton, Information Compliance Officer, Registrary's Office, James.Knapton@admin.cam.ac.uk, 01223 332331.

CHECKLIST OF ACTIONS

This checklist is arranged by target completion date. Some of the below actions will not be applicable in all Institutions. Consult the extended descriptions and rationales in the guidance notes as necessary. **A completed copy of the checklist should be returned to the Information Compliance Officer (James.Knapton@admin.cam.ac.uk) by 4 May 2018.**

Note Ref	Action required within each Institution	Target completion date	Complete [Y or N/A]
1.1	Check the University's updated core privacy notices supplied to student applicants, students, alumni/supporters, job applicants and staff	31 Dec 2017	
1.2	Delete any 'local' privacy notices you supply to student applicants, students, alumni/supporters, job applicants and staff	31 Dec 2017	
3.2	If you fundraise, amend your fundraising forms to include the Fundraising Promise	31 Dec 2017	
6.3(a)	Alert your staff to the University's data protection webpages	31 Dec 2017	
2.1	If you conduct outreach/student recruitment activity, amend your booking forms to refer to the updated CAO/GAO privacy notices for such events	31 Jan 2018	
2.3	If you use student personal information on the basis of consent, review/amend your consent mechanisms	31 Jan 2018	
3.1	If you use alumni personal information, amend your alumni update forms (if any) to refer to the CUDAR portal	31 Jan 2018	
4.2	Review/amend your procedures for engaging temporary workers or academic visitors	31 Jan 2018	
6.2	If you have a Departmental Data Protection Officer, amend their role title	31 Jan 2018	
7.1	If you publish student and/or staff profiles/photos on a public website, circulate an opt-out email to those students and/or staff	31 Jan 2018	
2.2	If you run any online services used by children under 13, implement a parental consent mechanism	28 Feb 2018	
3.3	If you send any direct marketing to alumni, liaise with CUDAR about marketing consents	28 Feb 2018	
6.4	If you run any CCTV systems, review/amend your signage and procedures	28 Feb 2018	
7.4	Alert your staff to the updated UIS information security guidance and training	28 Feb 2018	
2.5	If you hold records about unsuccessful student applicants and/or former students, review/amend your procedures for deleting them	31 Mar 2018	
4.1	Review/amend your procedures for procuring references for job applicants	31 Mar 2018	

4.3	If you hold records about unsuccessful job applicants and/or former staff, review/amend your procedures for deleting them	31 Mar 2018	
5.1	Alert your academic and research staff to the updated University guidance on research ethics and data protection	31 Mar 2018	
5.2	Alert your academic and research staff to the University guidance on research data management	31 Mar 2018	
6.1	If you have a Departmental Data Protection Policy, review/amend it (to align with the new University policy)	31 Mar 2018	
6.3(b)	Alert your staff to the updated University data protection training	31 Mar 2018	
7.2	Amend your website privacy policies (if any)	31 Mar 2018	
2.4	Amend your examination data retention policy (to align it with the updated University guidance)	30 Apr 2018	
3.4	Amend your privacy notices aimed at members of the public (if any)	30 Apr 2018	
3.5	If you send any direct marketing to members of the public, review/amend your consent mechanisms	30 Apr 2018	
6.5	Review/amend your records management and retention procedures	30 Apr 2018	
6.6	Review/amend your supplier contract arrangements with data processors	30 Apr 2018	
7.3	Add headline information about your key databases/systems/records to the new University Information Asset Register	30 Apr 2018	
7.5	Alert your procurement/IT staff to the new University guidance on privacy by design	30 Apr 2018	

GUIDANCE NOTES

The guidance notes are arranged thematically to aid distribution and discussion within Institutions.

Section 1 Core privacy notices

Ref	Action	Rationale	Target completion date
1.1	Check that the University's updated core privacy notices supplied to the following groups of people accurately reflect what you do with their personal information. If you use personal information in other ways, consult the Information Compliance Officer. (a) Student applicants and offer-holders https://www.information-compliance.admin.cam.ac.uk/data-protection/applicant-data (b) Students https://www.information-compliance.admin.cam.ac.uk/data-protection/student-data (c) Alumni and supporters (including non-alumni donors, prospective donors, and those joining museum membership/friend schemes) https://www.alumni.cam.ac.uk/data-protection (d) Job applicants https://www.hr.admin.cam.ac.uk/hr-staff/hr-data/applicant-data (e) Staff (including academic visitors, temporary workers, and affiliated teaching or research staff) https://www.hr.admin.cam.ac.uk/hr-staff/hr-data/how-we-handle-your-personal-data	Under the GDPR we need to supply individuals with detailed statements (usually 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. Institutions must not use information in other ways that individuals don't know about. If there are other uses, a supplementary privacy notice may need to be agreed with the Information Compliance Officer.	31 Dec 2017

1.2	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 Institutions will supply 'local' privacy notices to these groups (except, e.g., where Institutions are directly responsible for admissions or run major alumni programmes). 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.	31 Dec 2017

Section 2 Student applicants and students

Ref	Action	Rationale	Target completion date
2.1	Ensure that booking forms for student outreach/recruitment activities that you run contain links to http://www.undergraduate.study.cam.ac.uk/how-we-use-participant-data (undergraduates) or http://www.graduate.study.cam.ac.uk/events/how-we-use-participant-data (graduates). *Relevant staff should have already received guidance from CAO/GAO about this.*	See Section 1.1. These standard CAO/GAO privacy notices for outreach/recruitment events are comprehensive and ensure that all of the necessary topics are covered.	31 Jan 2018
2.2	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. *Suggested wording is given in Annex 2.*	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.)	28 Feb 2018
2.3	If you use students' personal information on the basis of those students' consent, check that you really need consent. If you	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	31 Jan 2018

	do, ensure the consent is a genuine free choice and is recorded. *Suggested wording is given in Annex 2.*	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).	
2.4	Ensure that your examination data retention policy is updated in line with the General Board's forthcoming updated guidance to be published at http://www.educationalpolicy.admin.cam.ac.uk/curricula-and-assessment/retention-examination-data. *Institutions will be advised as soon as the updated guidance is available.*	This guidance will be updated in minor ways to reflect the changes under the GDPR regarding students' access rights to their personal information. (The UK's Data Protection Bill – see Annex 1 – contains a provision that exam scripts will continue to be exempt from subject access rights.)	30 Apr 2018
2.5	Ensure that you have procedures in place to: (a) Delete or anonymise copies of unsuccessful student applications around 1 year after the completion of the relevant applications cycle. (b) Delete or anonymise the non-CamSIS records of former students around 6 years after their graduation/departure (unless you require them solely for research/statistical purposes).	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.	31 Mar 2018

Section 3 Alumni, supporters and public engagement

Ref	Action	Rationale	Target completion date
3.1	If you run any processes (e.g. webpages or forms) that ask your alumni to update their contact details, ensure that alumni are pointed instead to https://www.alumni.cam.ac.uk/contact/update-your-details.	A central principle of data protection legislation is to keep personal data accurate. The use of CUDAR's update portal ensures that the central record is accurate. Institutions will be advised by CUDAR of updates relevant to their specific alumni.	31 Jan 2018
3.2	If you manage any Institutional hard copy or online donation forms, ensure that they include the following text: **The Fundraising Regulator** We are registered with the Fundraising Regulator. Please read our fundraising promise at: https://www.alumni.cam.ac.uk/fundraising-promise	The Fundraising Regulator is a new UK regulatory body. The University (like all other HEIs) is registered and it is a mandatory condition of registration that the Fundraising Promise is included on focussed fundraising materials. While this change is not directly related to GDPR, it has been included in this document for the sake of completeness.	31 Dec 2017
3.3	If you send emails to alumni/supporters that class as unsolicited electronic direct marketing (i.e. emails promoting the University's aims and ideals, offering benefits or services, selling goods or advertising events, but not 'pure' e-newsletters or 'service' emails), make contact with CUDAR to ensure that the University holds an appropriate consent for each recipient.	While consent is not required under the GDPR either to hold personal information about alumni/supporters or to contact them by post, it is required in order to send them unsolicited electronic direct marketing, which is widely defined (under the Privacy and Electronic Communications Regulations 2003, as amended). CUDAR holds a record of consents obtained from alumni/supporters and these apply University-wide.	28 Feb 2018
3.4	If you collect personal information from members of the public (e.g. individuals booking to attend your events or signing up for newsletters about your research), review and revise the information you supply to them at the point you collect their data. *Suggested wording is given in Annex 2.*	See Section 1.1. The University does not have a core privacy notice for members of the public; 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, including through cross-referral to the 'fixed' statutory information at https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data.	30 Apr 2018

3.5	If you send emails to members of the public that class as unsolicited electronic direct marketing, ensure that you have collected and recorded their consent to do this. *Suggested wording is given in Annex 2.*	See Section 3.3. The suggested wording in Annex 2 ensures that consents are collected appropriately.	30 Apr 2018

Section 4 Job applicants and staff

Ref	Action	Rationale	Target completion date
4.1	Ensure that you follow standard University procedures (and use standard wording) when procuring references for job applicants (as outlined at https://www.hr.admin.cam.ac.uk/recruitment/step-3-recruit-and-select/request-references).	These templates 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.	31 Mar 2018
4.2	Ensure that you follow standard University procedures when engaging temporary workers through TES (as outlined at https://www.hr.admin.cam.ac.uk/hr-services/tes/information-those-requiring-temp) or hosting academic visitors (as outlined at https://www.hr.admin.cam.ac.uk/policies-procedures/visitors-agreements).	These procedures ensure that temporary workers/academic visitors are adequately informed of their confidentiality and data protection obligations (in ways that mirror staff employment contracts).	31 Jan 2018
4.3	Ensure that you have procedures in place to: (a) Delete or anonymise copies of unsuccessful job applications around 1 year after the completion of the relevant recruitment exercise. (b) Delete or anonymise the non-CHRIS records of former staff around 6 years after their departure (unless you require them solely for research/statistical purposes).	See Section 2.5.	31 Mar 2018

Section 5 Research

Ref	Action	Rationale	Target completion date
5.1	Ensure that your academic and research staff (especially Principal Investigators) are aware of the forthcoming updated guidance on research involving personal data to be published at https://www.research-integrity.admin.cam.ac.uk/ and https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance. *Institutions will be advised as soon as the updated guidance is available.*	The GDPR applies to personal data processed for academic and research purposes but there are significant exemptions from the standard provisions when: (a) processing personal data for academic purposes; or (b) processing personal data for research/statistical purposes. (The UK's Data Protection Bill – see Annex 1 – contains many of these exemptions.) Academic researchers will need to read the updated 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 updated guidance.	31 Mar 2018
5.2	Ensure that your academic and research staff (especially Principal Investigators) are aware of the guidance on research data management at http://www.data.cam.ac.uk/.	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). Certain research projects also may 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	31 Mar 2018

		involves sensitive information such as the health or ethnicity of the participants.	

Section 6 Institutional management

Ref	Action	Rationale	Target completion date
6.1	If you have issued a Departmental Data Protection Policy, review it against the forthcoming 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. *Institutions 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. We have not previously issued a University Data Protection Policy but have decided that we need one now.	31 Mar 2018
6.2	If you have designated a particular member of staff as your Departmental Data Protection Officer, change their role title.	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.	31 Jan 2018
6.3	Ensure that your staff: (a) Understand the fundamentals of data protection legislation, and especially the GDPR, by making them aware of https://www.information-compliance.admin.cam.ac.uk/data-protection (and linked pages). (b) Complete the forthcoming updated online University data protection training course.	Under the GDPR we need to demonstrate that we are following the law, and appropriate awareness-raising and training is one aspect of this.	6.3(a) 31 Dec 2017 6.3(b) 31 Mar 2018

	Institutions will be advised as soon as the updated online training course is available.		
6.4	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. *Suggested signage wording is given in Annex 2.*	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.	28 Feb 2018
6.5	Check that your records management and retention procedures are aligned with the forthcoming updated University guidance at https://www.information-compliance.admin.cam.ac.uk/records-management. *Institutions will be advised as soon as the updated guidance is available.*	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.	30 Apr 2018
6.6	Review your supplier arrangements with data processors. Arrangements with University-approved IT suppliers or major technology companies (e.g. Amazon Web Services, Apple, Microsoft, Google, Dropbox, SurveyMonkey, Qualtrics, MailChimp) 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 Information Compliance Officer of those arrangements.	Under the DPA there has always been a requirement for the University as a 'data controller' to ensure that its suppliers commit contractually to strong levels of information security when they act as 'data processors'. 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 DPA's requirements regarding transfers of personal data outside the EEA, and methods of ensuring that personal data are kept safe when this happens.	30 Apr 2018

	(b) Ensure that any contractual arrangements with your suppliers comply with the GDPR, in particular with regard to: (i) the general data protection obligations of the supplier; and (ii) the further data protection obligations of the supplier if they are based outside the EEA. *Advice on reviewing supplier contractual arrangements is given in Annex 2.*		

Section 7 Institutional IT

Ref	Action	Rationale	Target completion date
7.1	If you publish student and/or staff profiles (including photos) on a publicly available website (not an intranet or Lookup), ensure that those students and/or staff have been given an opportunity to opt-out of this. *Suggested wording is given in Annex 2.*	It is acceptable under both the DPA and the GDPR to publish such information about students and/or staff but first you should give them an opportunity to opt-out.	31 Jan 2018
7.2	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 forthcoming UIS guidance. Such policies sometimes are embedded in website terms setting out user obligations. *Institutions will be advised as soon as the guidance is available.*	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.	31 Mar 2018
7.3	Be ready, when prompted, to:	Under the GDPR the University needs to maintain records about the personal data we hold, how we use it, and how we keep it secure. The IAR is our way of fulfilling this compliance requirement. Entering information assets onto the register	30 Apr 2018

	(a) Enter headline information about your key databases/datasets/paper filing systems into the forthcoming University Information Asset Register (IAR). (b) Implement any remedial work concerning the handling and security of those databases/systems/paper filing systems that is prompted by this process. *Relevant staff should have been contacted and/or interviewed already by UIS in preparation for this. Institutions will be advised as soon as the IAR and associated documentation are available.*	(and, where appropriate, answering any associated questionnaires in doing so) will also allow Institutions to identify any information assets that have insufficient security depending on their risk profile (e.g. inappropriate access levels, lack of encryption of sensitive information or an inadequate backup routine) and which might require simple remedial actions. The IAR will also provide an overview of how different information assets are managed to assist with other aspects of GDPR compliance.	
7.4	Ensure that your staff understand information security requirements – including security incident (including personal data breach) reporting procedures – by making them aware of the resources and training modules at https://www.uis.cam.ac.uk/cybersecurity. *Relevant staff already should have been contacted already by UIS about this.*	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 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. Under the GDPR certain types of personal data breach have to be reported to the regulator (the ICO – see Annex 1) within 72 hours of discovery, and so staff need to know the right procedures to report and escalate breaches for investigation, containment and (where necessary) onward reporting.	28 Feb 2018
7.5	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, by following the forthcoming guidance to be published at https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance.	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	30 Apr 2018

	Institutions will be advised as soon as the guidance is available.	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) will apply in the UK and the rest of the EU from 25 May 2018 and will replace the Data Protection Act 1998 (DPA). The GDPR is designed to harmonise and strengthen data protection law and practice across the EU. Like the DPA, it will be regulated 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 a Data Protection Bill that was introduced in Parliament in September 2017 and will become law by May 2018; amongst other things, the Bill 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. Until the Bill receives Royal Assent, it remains subject to amendment.

2. Like the 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 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 'high risk' processing activities.

6. The GDPR and the UK Data Protection Bill currently before Parliament 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 Data Protection Working Group, chaired by the Registrary, to work on and oversee the University's preparations. As well as members from various UAS offices, University Information Services and the University Library, the Group includes representatives from academic departments, the Office of Intercollegiate Services, Cambridge Assessment and Cambridge University Press to ensure a coordinated approach to the implementation of the changes across Collegiate Cambridge.

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 Cambridge is a devolved University, some changes are required at Institution level. This document is designed to guide Institutions in thinking about the changes they will need to make and how they might implement them.

Further information

10. See https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation.

ANNEX 2 SUGGESTED TEMPLATE WORDINGS

These wordings are suggestions. Institutions 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
2.2	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.
2.3	Wording for student consent to specific data use	Please [sign/electronically sign/tick], date and [return by UMS/return by email/submit] the below declaration: I consent to the [Institution name] using my personal data for [describe the specific purpose] and understand that I can withdraw my consent at any time.
3.4	Wording when collecting personal information from members of the public	[In addition to a link to the University's generic webpage, the topics that need to be covered are as follows: the purpose of the personal data use; the legal basis of the personal data use; information about data sharing and international transfers; whether there is any statutory or contractual need to supply any personal data; whether any automated decisions are taken based on the personal data that might affect the individual; and – if also collecting information from other sources – the categories and sources of those personal data. It is considered unlikely that many of these will apply to most Institutions and the below simple example, which deliberately does not cover all of these topics, is likely to suffice for most situations; please contact the Information Compliance Officer if your situation is more complex.] <u>How the University Hairdressing Service uses your personal information</u> The University Hairdressing Service uses your personal information to keep booking records and to contact you to let you know when your next haircut is due. We use your personal information in order to deliver our contractual obligations to you as a user of our service. Our standard terms of service are available from our website https://www.hairdressing.admin.cam.ac.uk/. We share your personal information with a local salon, Tasteful Beauty Cambridge, if you ask for other services (e.g. manicures) that we do not offer ourselves.

		For more information about how we handle your personal information, and your rights under data protection legislation, please see https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data.
3.5	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
6.4	Wording for CCTV signage	The University of Cambridge operates CCTV on these premises for the purposes of safety and security. For further information please phone [contact number].
6.6	Contractual review checklist	The contract (or terms of business) with a third party supplier (a Processor) that processes personal data on behalf of the University (the Controller) needs to cover the following: • Details of the subject matter, duration, nature and purpose of the processing, and the type of personal data and categories of data subject. • That the Processor must only act on the written instructions of the Controller (unless required by law to act without such instructions). • That the Processor must ensure that people processing the data are subject to a duty of confidence. • That the Processor must take appropriate measures to ensure the security of processing. • That the Processor must only engage a sub-processor with the prior consent of the data controller and a written contract. • That the Processor must assist the Controller in providing subject access and allowing data subjects to exercise their rights under the GDPR. • That the Processor must assist the Controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments. • That the Processor must delete or return all personal data to the Controller as requested at the end of the contract. • That the Processor must submit to audits and inspections, provide the Controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the Controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

		In addition, if the Processor is based outside the EEA, the Controller needs to ensure *either* that the Processor is based in a country deemed by the EU to offer 'adequate' data protection standards (including companies covered by the EU-US Privacy Shield) *or* that the Processor has signed up to/will sign specific model contractual clauses issued by the EU. Institutions are encouraged to seek advice from the Legal Services Office or the Information Compliance Officer if in doubt.
7.1	Wording for website profile publication opt-out	We would like to include your [name/contact details/research profile/photo] on our publicly accessible website at [URL]. Please let us know by [date] if you do not wish some or all of your details to be included.