DON'T PANIC
TechLink Seminar

GDPR - General Data Protection Regulation: Implications for UIS

Madeleine Taylor
Information Services Compliance Officer, UIS

Wednesday 14th February 2018
Working together for excellence in education, research and operations through Information Services
Context 1

The obligations of the GDPR fall onto the University as an institution and as a Data Controller NOT on individuals.

An individual cannot be sanctioned by the GDPR except for wilful damage etc.

The way individuals can help the University not to be sanctioned is to follow the instructions given by the University.

The UIS has two roles in terms of GDPR:

• As a ‘department/office’, like any other NSI, Department or UAS office

• As a provider of services to various parts of the University
Context 2

There is **nothing mandated** in the Regulation in terms of **technology**.

There is **no precedence** of court rulings using the GDPR.

There is some help from the Working 29 party in EU and some guidance papers from the Information Commissioner’s Office (ICO) in various areas of the GDPR **but not on technology**.
I would like to introduce/explain a little about

- the Regulation itself
- What the University has already done, has already planned and is doing about getting the University compliant with GDPR
- What the UIS has already done, has already planned and is doing about following what the University want us to do
- What the UIS still needs to do
- What the UIS has done, has planned and is doing to help institutions
WHAT IS THE GDPR?
REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 21 thereof,
Having regard to the proposal from the European Commission,
After transmittal of the draft legislative act to the national parliaments,
Having regard to the opinion of the European Economic and Social Committee (1),
Having regard to the opinion of the Committee of the Regions (1),
Acting in accordance with the ordinary legislative procedure (1),

Whereas:

GDPR

{{re-gu-lay-shun}}

Mostly harmless _

Earth

{{lang-la|Terra}}

Mostly harmless _
What is the GDPR?

EU General Data Protection Regulation applies *in full* from 25 May 2018

Data Protection Act 1998 repealed on same date

Will apply in UK despite Brexit;

Enhanced and more prescriptive standard of data protection law

Based around existing concepts of data protection principles and data subject rights
Types of Personal Data

Personal Data

- Any information relating to an identified or identifiable natural person (‘data subject’) – but not those who are deceased

- The identifier such as a name, an identification number, location data, an online identifier...

- GDPR includes IP Addresses in the list of identifiers

Special category data (sometimes called Sensitive Personal Data)

- Racial / ethnic origin, political opinions, religious / philosophical beliefs, trade union membership, genetic data, biometric data, health, sex life / sexual orientation

- Need to meet an additional legal basis – e.g. with explicit consent
Article 5 (1) Data Protection Principles

- Fairly and lawfully
- Securely using appropriate technical and organisational measures
- For a specific legitimate purpose
- Not for longer than is needed
- Not more than is needed
- Accurate and up-to-date
Data Controller must be able to demonstrate compliance
New Focus in GDPR on Accountability

• Policies and procedures for data protection by design and by default

• Detailed rules surrounding contracts with joint data controllers and with data processors

• Maintenance of a detailed personal data register

• Certain personal data breaches to be notified to ICO within 72 hours

• Newly prescribed Data Protection Impact Assessments for ‘high risk’ processing

• Newly prescribed senior role of Data Protection Officer

• Extra requirements for Privacy Notices
WHAT THE UNIVERSITY has already done
has already planned
and is doing
ABOUT GETTING THE UNIVERSITY COMPLIANT WITH GDPR?
The University has...

- Set up GDPR Working Group chaired by Emma Rampton
- High Level plan from GDPR-WG ‘owned’ by James Knapton
- Vijay Samtani as UIS representative on GDPR-WG
- Madeleine Taylor Certified GDPR Practitioner working closely with James Knapton and GDPR-WG
- Toolkit by GDPR-WG sent by James Knapton to all HoDs, D.A.s, Heads of central offices. On the back there is a ‘checklist’ to tick off jobs once they’re done.
### GDPR WG Plan

#### Part A - Changes to policies and procedures

<table>
<thead>
<tr>
<th>Category</th>
<th>Output</th>
<th>Legal reason for Output</th>
<th>Activity</th>
<th>Working Group Lead on Activity</th>
<th>Other Working Group members involved in Activity</th>
<th>Target completion date of Activity</th>
<th>Internal prerequisites before activity can commence</th>
<th>Risk profile of Activity (URMIR)</th>
<th>Notes of Activity at date of plan's last revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.1 Identify activities (e.g. outreach) where the University engages with child pre-applicants online</td>
<td>Jan Bleed</td>
<td>James Kingston, Matthew Russell</td>
<td>June 2017</td>
<td>None</td>
<td>N/A</td>
<td>Complete</td>
</tr>
<tr>
<td>1.2</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.2 Ensure consent privacy notices and consent mechanism are used for standard and non-standard (e.g. EIE, EDD, EME) admissions areas</td>
<td>Jan Bleed</td>
<td>James Kingston, Matthew Russell</td>
<td>December 2017</td>
<td>Completion of EU</td>
<td>L</td>
<td>Complete</td>
</tr>
<tr>
<td>1.3</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.3 Implement amended and standardized data notice and consent mechanism for all areas of student application</td>
<td>James Kingston</td>
<td>Matthew Russell</td>
<td>January 2018</td>
<td>Completion of U12113</td>
<td>L</td>
<td>Complete</td>
</tr>
<tr>
<td>1.4</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.4 Draft and publish amended main privacy notice for students</td>
<td>Jon Board</td>
<td>Matthew Russell</td>
<td>July 2017 (onward)</td>
<td>Completion of 12.112</td>
<td>N/A</td>
<td>Complete</td>
</tr>
<tr>
<td>1.5</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.5 Draft and publish amended main privacy notice for students</td>
<td>James Kingston</td>
<td>Alice Ewing, Rosemary Boyle</td>
<td>June 2017</td>
<td>None</td>
<td>N/A</td>
<td>Complete</td>
</tr>
<tr>
<td>1.6</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.6 Draft and publish amended main privacy notice for students</td>
<td>Matthew Russell</td>
<td>Jon Board, Rosemary Boyle, James Kingston</td>
<td>November 2017</td>
<td>None</td>
<td>N/A</td>
<td>Complete</td>
</tr>
<tr>
<td>1.7</td>
<td>Amended and standardized data notice for pre-applicants (e.g. student enrollment event attendance) to cover processing both by the University and the Colleges, including new parental consent mechanism for the continuing use of pre-applicant data of those under the GDPR</td>
<td>Newly prescribed privacy notice content (Art. 13-14) and new mechanism for processing of children's online data (Art. 15-16)</td>
<td>1.7 Draft and publish amended main privacy notice for students</td>
<td>James Kingston</td>
<td>Jon Board, Rosemary Boyle, Matthew Russell</td>
<td>June 2017</td>
<td>None</td>
<td>N/A</td>
<td>Complete</td>
</tr>
</tbody>
</table>

---

**Working together for excellence in education, research and operations through Information Services**

---

**University of Cambridge**

---
So, from the GDPR-WG, we had this to do....

1. Information Asset Register
2. GDPR Checklist for UIS systems
3. Personal Data Breach Response Procedure
4. Building Data Protection By Design into our project and solutions
5. Privacy Notices
6. Review of UIS Contracts for GDPR compliance
7. Revisions to our Online Information Security Training
8. Update Information Security Policies
To: Departmental Administrators (and equivalents).
Copied to: Heads of Institutions; Heads of Schools; Secretaries of Schools; Members of the University’s GDPR Data Protection Working Group.

Dear colleagues,

Purpose and background

The purpose of this email is to alert you to the attached toolkit which has been designed to assist University Institutions in implementing their preparations for the General Data Protection Regulation (GDPR).

The GDPR is a new law ... (that) requires the University, both centrally and within Institutions, to make a number of changes as to how we collect, hold and use information about living identifiable individuals ...

The changes we need to make are not optional – they are requirements to ensure that the University complies with the new law. ...

... https://www.information-compliance.admin.cam.ac.uk/data-protection/general-data-protection-regulation (Raven required),
GDPR Toolkit

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

Pages 2 to 3  
Checklist of actions
The checklist is comprehensive but not all actions apply to all Institutions. The checklist includes target completion dates so as to stagger the work. **Institutions are strongly encouraged to convene a group of colleagues, led by the Departmental Administrator (or equivalent) and including the Computer Officer (or equivalent), and to begin work as soon as possible. A completed copy of the checklist should be returned to the Information Compliance Officer (James.Knapton@admin.cam.ac.uk) by 4 May 2018.** Workshops have been arranged to assist.

Pages 4 to 14  
Guidance notes
The guidance notes, arranged in thematic sections to aid distribution and discussion, support the checklist and include a short legal rationale for each action. Many of the actions simply require Institutions to check certain documentation and confirm that their current practices do not conflict. Others require the amendment of existing processes/documentation (or the deletion of duplicates). Some colleagues (e.g. Computer Officers) are likely to be aware of certain actions already. The guidance notes identify those occasions where actions are contingent upon forthcoming further documentation or guidance.

Pages 15 to 17  
Annex 1: Key facts about the GDPR and the University’s preparations
This annex gives legal background and information about the University’s GDPR Data Protection Working Group.

Pages 18 to 20  
Annex 2: Suggested template wordings
This annex gives suggested template wordings to be used when fulfilling some of the (cross-referred) actions.

CONTACT FOR QUESTIONS

UNIVERSITY OF CAMBRIDGE
Working together for excellence in education, research and operations through Information Services
GDPR Toolkit

GUIDANCE NOTES

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

Section 1 Core privacy notices

<table>
<thead>
<tr>
<th>Ref</th>
<th>Action</th>
<th>Rationale</th>
<th>Target completion date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>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.</td>
<td>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.</td>
<td>31 Dec 2017</td>
</tr>
</tbody>
</table>

Section 7 Institutional IT

<table>
<thead>
<tr>
<th>Ref</th>
<th>Action</th>
<th>Rationale</th>
<th>Target completion date</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>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.</td>
<td>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.</td>
<td>31 Jan 2018</td>
</tr>
</tbody>
</table>

Suggested wording is given in Annex 2.

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.

<table>
<thead>
<tr>
<th>Note Ref</th>
<th>Action required within each Institution</th>
<th>Target completion date</th>
<th>Complete[Y or N/A]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Check the University’s updated core privacy notices supplied to student applicants, students, alumni/supporters, job applicants and staff</td>
<td>31 Dec 2017</td>
<td>Y</td>
</tr>
<tr>
<td>1.2</td>
<td>Delete any ‘local’ privacy notices you supply to student applicants, students, alumni/supporters, job applicants and staff</td>
<td>31 Dec 2017</td>
<td>Y</td>
</tr>
<tr>
<td>3.2</td>
<td>If you fundraise, amend your fundraising forms to include the Fundraising Promise</td>
<td>31 Dec 2017</td>
<td>Y</td>
</tr>
<tr>
<td>6.3(a)</td>
<td>Alert your staff to the University’s data protection websites</td>
<td>31 Dec 2017</td>
<td>Y</td>
</tr>
<tr>
<td>2.1</td>
<td>If you conduct outreach/student recruitment activity, amend your booking forms to refer to the updated CAO/GAO privacy notices for such events</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>2.3</td>
<td>If you use student personal information on the basis of consent, review/amend your consent mechanisms</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>3.1</td>
<td>If you use alumni personal information, amend your alumni update forms (if any) to refer to the CUDAR portal</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>4.2</td>
<td>Review/amend your procedures for engaging temporary workers or academic visitors</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>5.2</td>
<td>If you have a Departmental Data Protection Officer, amend their role title</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>7.1</td>
<td>If you publish student and/or staff profiles/photos on a public website, circulate an opt-out email to those students and/or staff</td>
<td>31 Jan 2018</td>
<td>Y</td>
</tr>
<tr>
<td>2.2</td>
<td>If you run any online services used by children under 13, implement a parental consent mechanism</td>
<td>28 Feb 2018</td>
<td>Y</td>
</tr>
<tr>
<td>3.3</td>
<td>If you send any direct marketing to alumni, liaise with CUDAR about marketing consents</td>
<td>28 Feb 2018</td>
<td>Y</td>
</tr>
<tr>
<td>3.4</td>
<td>If you run any CCTV systems, review/amend your signage and procedures</td>
<td>28 Feb 2018</td>
<td>Y</td>
</tr>
<tr>
<td>7.4</td>
<td>Alert your staff to the updated UIS information security guidance and training</td>
<td>28 Feb 2018</td>
<td>Y</td>
</tr>
</tbody>
</table>
Toolkit for UIS as a department (Institutional IT Section)

So there are 5 main IT bits for us:

1. Notification regarding publishing photos on public website
2. Privacy Notices
3. Populate the Information Asset Register when asked to
4. Inform staff of Information security response including personal data breach response procedure
5. Data protection by design in the procurement or new build process
WHAT THE UIS has already done has already planned and is doing ABOUT GETTING THE UNIVERSITY COMPLIANT WITH GDPR?
So, from the GDPR-WG, we had to do these things....

1. Information Asset Register
2. GDPR Checklist for UIS systems
3. Personal Data Breach Response Procedure
4. Building Data Protection By Design into our project and solutions
5. Privacy Notices
6. Review of UIS Contracts for GDPR compliance
7. Revisions to our Online Information Security Training
8. Update Information Security Policies
1 Information Asset Register

ACTION

- Interviews with DAs and COs across University
- Visibility raised at interviews about Admin Information Assets, the IAR and GDPR

RESULT

- Initial view of Information Assets and issues in rolling out IAR
- An Initial Information Asset Register has some degree of population, albeit quite sparse

FURTHER ACTION

- Use this to populate IAR as initial pass
2

GDPR Checklist
(Covering Technical and Organisational Measures)

**ACTION**
- UIS System Security Checklist (SSC)
- GDPR Checklist for UIS systems
- Institutional Maturity Model

**RESULT**
- **Completed** the SSC against 5 major UIS systems (CamSIS, X5, CHRIS, EDMS, Moodle)
- **Completed** GDPR Checklist against some UIS and some UAS systems (11)
- Institutional Maturity Model in draft form
- **Rolled-out** SSC and GDPR Checklist

**FURTHER ACTION**
- **Re-writing** SSC and GDPR Checklist for use, if wanted, by Institutional DAs and COs
- Further UIS systems to be completed.
- Creation of **guidance documents** for bits missing.
UIS System Security Checklist

UIS System Checklist (UIS Use only)

Hi Taylor, when you submit this form, the owner will be able to see your name and email address.

* Required

1. Please provide the name of the system this checklist relates to *

   Enter your answer

2. Does a System Management Committee exist?

   Guidance Notes:
   A System Management Committee should be in place to consider and sign off policies, processes and procedures of Tier 1 services. They should ensure that there is due diligence in reviewing these for all Tier 1 services. They should maintain defined Terms of Reference, Roles and Responsibilities and minutes of meetings.

   ○ Yes
   ○ No
GDPR Checklist for UIS Systems

EU GDPR System Checklist for UIS Systems

This checklist is to be used to record the ability of a system to comply with the EU General Data Protection Regulation (GDPR). It is envisaged that it will be completed by UIS Service Managers with some collaboration with the Information Owners or major users of the system.

The checklist itself contains 44 Questions but you may not see all of them. This is because it is dynamic so questions appear depending on your previous answer. You will need to answer the last question at the bottom to see the next question appear. Remember there will be at least 30 for you to complete the form.

When you click Submit, you will receive an email giving you the results of your submission.

Definitions are here: https://www.information-compliance.admin.cam.ac.uk/files/gdpr_definitions.pdf

Further Support is available here uis-compliance@uis.cam.ac.uk Madeleine Taylor, UIS

Hi Madeleine, when you submit this form, the owner will be able to see your name and email address.

Required

1

Please enter your preferred name for correspondence purposes (e.g. Liz Dr Richard Smith) *
13. Accuracy of the data: Spot Checks

14. Accuracy of the data: Changes

15. Accuracy of the data: Verification
Data Protection by Design (DPbyD)

ACTION

• DPbyD into Project Board Process
• Engagement with Procurement

RESULT

• Project Board and Processes already including DPbyD

PLAN

• Await DPO on final version of Data Protection Impact Assessments (DPIAs) but in meantime doing Mini-DPIAs
**ACTION**

- Main Site Privacy Notice [www.cam.ac.uk](http://www.cam.ac.uk) completed
- Privacy Notice Structure written and agreed by JK

**RESULT**

- Structure enables easy to write and streamlined privacy notices

**PLAN UIS**

- ‘Specific’ Privacy Notice to be written and approved as model
- Re-work or pull-down all UIS Privacy Notices
3, 6, 7, 8  Breach Procedure, Contracts, Training & Policies

**ACTION**
- **UIS contracts** have been listed, checked and re-listed with staff allocated.
- **Incident Procedure** already completed

**PLAN WG**
- JK to write **Data Protection Policy**
- JK to write **DP Training**

**PLAN UIS**
- **UIS staff** to check **contracts** list for relevance and then rework to fit GDPR requirements
- **Rewrite** of Incident Page to include **Personal Data Incidents**
- **Information Security Training** to reference Data Protection Training and Breach Notification
- **Update Information Security Policies**
WHAT DOES UIS STILL HAVE TO DO?
UIS as a ‘department’

UIS have to answer questions asked of it, by James Knapton and the GDPR Working group, just like every other department
What UIS still need to do

- **Service Managers** know about the Information Asset Register and will get access to the University-wide one once it is launched.

- **Madeleine Taylor** has just written the new ‘specific’ privacy notice where data is entered by the data subject and had it approved by James Knapton.

- **Vijay Samtani (CISO)** is organising a web page for information on GDPR and also information security and personal data breach response procedure to replace the one linked to in JK notes to make it all clearer and easier.

- **James Knapton** is writing the Data Protection Policy for the University and then we will link with this for our web-pages and training.
Summary: What UIS Service Managers are doing...

1. Updating the new Information Asset Register (IAR) by e/o April
2. Doing System Security Checklist for each of their system(s)
3. Doing GDPR Checklist for their system(s) on data held to run their system; not the data put on by other institutions.
4. Finding all their contracts
5. Rewriting their privacy notices ready, if relevant
WHAT IS UIS DOING TO HELP THE IT COMMUNITY WITH THEIR COMPLIANCE?
What is UIS doing to help institutions with their compliance?

- Information Asset Register
- System Security Checklist for non UIS systems
- GDPR Checklist for non UIS systems
- Privacy Notices
- Presentations
Information Asset Register (IAR)

**ACTION**
- **Information Asset Project** is now:
  - **Information Asset Register Project**

**RESULT**
- **Sponsor** is Emma Rampton, delegated to James Knapton
- **Project Board:** James Knapton, John Norman, Vijay Samtani, Gillian Weale
- **Project Plan** completed
- **Prototyping** now done;
- **Build** being done. On **Sprint** 2 of 4

**FURTHER ACTION**
- **Pilot** mid February to March.
- **Launch & Rollout** in late March
- **Handover to Operations** in late April
Institution System Security Checklist (not UIS systems)

This checklist is to be used by Computer Systems Administrators at an institution, to record the system-specific and department-specific information about a system or the system itself.

If you would like further information on a particular item, please contact:

Thanks and kindest regards,
Maddy

Madeleine Taylor
Information Services Compliance Officer

30  Malware Protection

Do all servers running this system/service have up-to-date anti-malware installed and running on them?

☐ Yes
☐ No

31  Operational Processes: Documented Operational Processes and Procedures

Are documented operational processes in place that have been appropriately agreed?

Guidance Notes:
Documented Operational Processes to be written by the Systems Manager covering all aspects in detail including roles and responsibilities, signed off by the Committee/Head of Institution and reviewed on an annual basis for Extremely Important systems.
For other systems, an outline operational processes to be written by the Systems Manager covering relevant details, signed off by the Information Asset Owner and reviewed when necessary.

Hi Madeleine, when you submit this form, you will be required to enter your name. This is a required field.

* Required
EU GDPR System Checklist

This checklist is to be used to help organisations comply with the General Data Protection Regulation (GDPR).

It is envisaged that it will be completed by data protection officers and Information Management Institutions with some collaboration from the Information Manager.

The checklist itself contains 44 Questions and additional questions appear depending on your responses. Remember to see the next question appear. Remember to add spaces to help with the automatic checking of your responses. Remember to save your progress when you click Submit, you will receive a link to your responses.

Definitions are here: https://www.info.gov.uk

Further Support is available here: un

Hi Madeleine, when you submit this form, please ensure that you have saved your work before closing.

* Required

---

19

Data Retention: Inspection Process

Please describe the process and frequency.

Enter your answer

---

20

Rights of the Data Subject: Access *

Can you extract all of the data about the data subject from this system within 1 month?

This question is checking the technical capabilities of the system rather than whether or not the right ought to be executed in any particular instance; that decision will rest ultimately with the University’s Data Protection Officer who will consult with relevant legal and technical colleagues as necessary.
You can download your own checklists from here....

Institution System Security Checklist: www.uis.cam.ac.uk/systemsecuritychecklist

Institution GDPR System Checklist: www.uis.cam.ac.uk/gdprsysteemchecklist

Definitions:
https://www.information-compliance.admin.cam.ac.uk/files/gdpr_definitions.pdf
Privacy Notices

**ACTION**
- Main Site Privacy Notice [www.cam.ac.uk](http://www.cam.ac.uk) drafted and agreed by JK
- Privacy Notice Structure written and agreed by JK

**RESULT**
- Structure enables easy to write and streamlined privacy notices

**PLAN UIS**
- ‘Specific’ Privacy Notice to be written and approved as **model** for all institutions
- Re-work or pull-down all UIS **Privacy Notices**
Specific Privacy Notice 1

Introduction
This page explains what personal information we gather when you visit the specific website within the University of Cambridge domain called The Newton Trust Small Grants Application.

Who will process my personal information?
The information published here applies to the use of your personal information (also known as ‘personal data’) by the University of Cambridge through the viewing or use of this site.

General personal information collected on our websites
When you visit any of the websites within the Cambridge domain we hold certain information about you for service and security reasons. For more information on this, please see https://www.cam.ac.uk/about-this-site.

Specific personal information collected on this website
This site asks you to provide information about yourself in a form.

We gather this information so that we can process your application and make judgements about your suitability for an award. We use this personal data to fulfil our ‘contractual’ relationship with you as an applicant or award-holder.

We share your data with the Newton Trust for them to evaluate your application and make a decision on the award they may be able to offer you.

We will collect data about you from the people you list as your referees to verify your identity and suitability.

We will hold your data for 5 years after application, whether or not you receive an award.

Further information
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.

This page was last updated in February 2018.
Presentations

Presentations have been given to some (mostly IT) groups:

1) University Library IT
2) Engineering IT
3) CRUK IT department
4) Research Data Management Group
5) Techlink Community Presentation is booked for Wed 14th Feb at 2pm

Including topics such as: GDPR, what the University is doing; what the UIS is doing; Data Protection by Design; Processor Contract requirements; the difference between anonymization and pseudonymisation wrt test data.
Further Information

James Knapton – Information Compliance Officer (Registry)

Compliance website: https://www.information-compliance.admin.cam.ac.uk

Retention Schedule: https://www.information-compliance.admin.cam.ac.uk/files/cambridge_master_records_retention_schedule.pdf

Data Protection pages: https://www.information-compliance.admin.cam.ac.uk/data-protection