UNIVERSITY OF CAMBRIDGE
Governance and Compliance Division

INFORMATION COMPLIANCE OFFICE

DATA PROTECTION – ANNUAL COMPLIANCE CHECKLIST FOR UNIVERSITY DEPARTMENTS, 2021-22

Summary

- This Checklist sets out a number of practical 'housekeeping' actions to be completed on an annual basis by individual University departments to help ensure their ongoing compliance with data protection law. This second version of the Checklist, for 2021-22, contains some updates and additional topics, in part arising from a survey about its use conducted in summer 2021.
- **Completion of the Checklist is mandatory in 2021-22. Departments are asked to submit a completed copy to data.protection@admin.cam.ac.uk by Friday 29 April 2022.**
- Work on the actions in the Checklist should normally be coordinated by the Departmental Administrator (or equivalent), working in collaboration with their departmental colleagues as necessary.

Version 2, issued November 2021

Guidance notes

Purpose of the Checklist

1. This Checklist sets out a number of practical 'housekeeping' actions to be completed on an annual basis by individual University departments (meaning any academic Faculty or Department within one of the six Schools, Non-School Institutions, and UAS Divisions) to help ensure their ongoing compliance with data protection law. This second version of the Checklist, for 2021-22, contains some updates and additional topics, in part arising from a survey about its use conducted in summer 2021.

2. Data protection law principally comprises the UK General Data Protection Regulation and the Data Protection Act 2018. This legislation, with some minor changes arising from the UK's exit from the EU, has been force since May 2018 and is regulated by the Information Commissioner's Office as well as the courts. All departments made substantial efforts to prepare themselves for the new legal regime through the completion of actions within a

GDPR Toolkit, but those efforts need to be supplemented by ongoing tasks to ensure that data protection compliance remains up-to-date and operationally embedded within each department.

Timings

3. **Completion of the Checklist is mandatory in 2021-22. Departments are asked to submit a completed copy, signed by the Departmental Administrator and the Head of Department (or equivalents), to data.protection@admin.cam.ac.uk by Friday 29 April 2022** (being the end of the first week of Full Easter Term)**.**

4. It is recognised that some departments might not have been able to complete all the actions by that point in the academic year. Where necessary, the submitted copy of the checklist can indicate that actions are ongoing and are intended to be completed by the end of the 2021-22 academic year. It is nonetheless hoped that, as this is the second year of the Checklist's operation, the checks required to fulfil some of the individual actions will have been carried out previously and accordingly re-completing them should be straightforward.

5. Completion of all the actions in the Checklist should take up to one full day of work, though it is envisaged that departments will choose to fulfil the individual actions gradually. Many actions are very straightforward and can be completed swiftly (e.g. circulating copies of guidance links), while others may already take place as part of routine business (e.g. destruction of old records). Not all actions will be applicable for all departments.

Practicalities

6. Work on the actions in the Checklist should normally be coordinated by the Departmental Administrator (or equivalent), though in some departments responsibility for data protection matters may have been given/delegated to a designated member of staff.

7. The Departmental Administrator (or other member of staff coordinating this activity) should do the following before starting work on the Checklist:

   (a) Speak to their Head of Department (or equivalent). This is because, under the University's Data Protection Policy approved by the Council, the Head of Department is responsible for data protection compliance within their department.

   (b) Identify key members of departmental staff to assist in working through the Checklist (e.g., as appropriate and insofar as the roles/functions exist, departmental staff responsible for local IT, HR, alumni relations, office management, student administration or purchasing).

   (c) Remind themselves of the core aspects of data protection compliance by reading the University's overview webpage on the topic.

8. Departmental Administrators and Heads of Department are asked to sign the Checklist before submitting it.

Guidance and advice

9. The Checklist refers as appropriate to specific parts of the University's extensive webpages on data protection and other pages containing University policies and guidance of relevance to this compliance area.

10. Advice may be sought from the Information Compliance Office (data.protection@admin.cam.ac.uk). Advice can be given not only on legal compliance matters, but also on the practical scope of the actions within a particular departmental context and/or on creating plans about how to tackle them.

11. Virtual workshops and/or advice drop-in sessions about the Checklist are being planned for early 2022; details of these will be communicated nearer the time.

Checklist

Topic	Action	Notes	Complete (where applicable). Add comments as necessary, especially if work is ongoing.
1 Training and guidance	Send an email to all departmental staff: • Asking those who have not completed the online data protection training course in the past 2 years to re-complete it. • Reminding all departmental staff of the most important University data protection resources as follows: o the Data Protection Policy. o the Data Protection Quick Guide. o the information about how to report personal data breaches. • Highlighting the following specialist guidance for specific types of departmental staff (as applicable): o the guidance on academic research and personal data for Principal Investigators and other researchers. o the guidance on data sharing for those involved in any purchasing/outsourcing decisions.	It is important to keep data protection training and awareness up-to-date and an annual reminder email is key to this. While a group email should suffice in most cases, Departmental Administrators and others with access to departmental University Training Booking System records can check on online training course completions within their department if desired, so as to approach staff on an individual basis. Individuals can also check their own training course completions on UTBS. The headline page of guidance on academic research and personal data includes links to detailed guidance on various topics, including participant information sheets, consent forms, data management plans, research data risk assessments, and data sharing provisions within research contracts.	
2 Information Asset Register	(a) Review, and as necessary update, your department's entries on the University's Information Asset Register.	The Information Asset Register (IAR) contains headline details about all information assets in use across the University. It helps to meet a core data protection accountability requirement as well as to assess	

	(b) Email Principal Investigators in your department to ask them to add/update any entries for their core research information assets to supplement the department's administrative ones.	information security risks. The IAR guidance page should assist with the process of reviewing entries; it also contains practical information about adding other users of the IAR within your department. Users can download a .csv report of all their department's entries once they are logged into the IAR in order to assist with the process of reviewing them.	
3 Records management	Use the guidance in the Master Records Retention Schedule to review records retention arrangements within your department, and dispose of records that are neither actively used, nor need to be retained for set periods, nor designated for permanent preservation. While departments should try to check their records retention arrangements across all areas of activity, it is especially important to focus on records about individual former students and members of staff (e.g. student or personnel files) to ensure that these are not being retained unnecessarily. Sections 2 and 6 of the Schedule are directly relevant in this regard.	Records are defined as all documents and materials, regardless of format, which facilitate the activities carried out by the University. These records may be created, received and maintained in hard copy, electronically (including emails), or both. Most departments will already have an annual record-keeping review/disposal process. For the purposes of data protection compliance, it is especially important to focus on operational records about individual former students and members of staff (e.g. student or personnel files). Normally, these do not need to be retained within departments for more than 6 years after the individual has left the University. (Core central records, including on CamSIS/CHRIS, are retained indefinitely.)	
4 Core privacy notices	(a) Read through the University's core privacy notices for students, for staff and for alumni to ensure that, in broad terms, they encompass the ways in which your department handles the personal data of those types of individual. (b) If you think that your department is handling the personal data of students, staff or alumni in any ways not broadly outlined within the core notices, seek advice from the Information Compliance Office. You may need to issue a 'supplementary' privacy notice.	A key aspect of data protection compliance is being open and honest with people about how you are using their personal information. The core privacy notices for students, staff and alumni are fundamental to fulfilling this requirement and it is important that they are accurate and supplemented where necessary.	

5 Website privacy policy	Check that your departmental website contains either (i) a link to main University website privacy policy or (ii) its own standalone privacy policy.	Website users need to be supplied with a privacy notice (often known in this context as a privacy policy) explaining how their personal information (e.g. their IP address) will be used when visiting that website. Because of the multiple website templates and content management systems in use across the University, departmental websites need to ensure that they either contain a link to the main website privacy policy or carry their own privacy policy. Guidance on this is available, which explains which option should be put in place.	
6 Local privacy notices	If, as a department, you run events or initiatives aimed at members of the public, check that a 'local' privacy notice has been issued to the participants explaining how their personal data will be used. This may be delivered as part of an online booking form, contract, brochure, email or any other appropriate method given the type of interaction.	The guidance on writing local privacy notices explains how you can link to a general webpage containing much of the statutory information these notices need to contain. This means that the topics to be covered within your local notice can be brief and factual (often no longer than three or four sentences).	
7 Electronic marketing	If, as a department, you run any email lists that would class as direct electronic marketing (e.g. lists for alumni or members of the public about departmental events) check that the recipients have consented to the receipt of those emails and that there is a simple 'unsubscribe' option included on each email.	The guidance on direct marketing should be read carefully to ensure that your list really does class as direct electronic marketing. The guidance explains some of the legal complexities about sending direct marketing to different types of email address. In short, departmental email lists aimed at departmental (or wider University) students or staff usually will *not* class as direct electronic marketing, and definitely will not do so if the list is used for informational announcements that the students/staff need to know. Efforts accordingly should be focused on email lists aimed at departmental alumni and members of the public.	
8 Website profile pages	Ensure that all newly starting departmental students and staff have been given the opportunity to opt out of appearing on *publicly accessible* departmental webpages, such as listings or standalone profile pages. This opportunity could be mentioned in a group email, an	Nearly all University students and staff are happy to have their name, contact details, profile and photo published on a publicly accessible departmental website. However, all new starters should be given the opportunity to opt out of this. (Note that all departmental staff and students can be	

	announcement in a departmental newsletter or welcome session, an item in a departmental new starter induction form, or any other communication method.	included in internal listings, directories and intranet pages.)	
9 Suppliers handling personal data	Review any *new* arrangements that have been made within the department that involve third party suppliers handling personal data on your behalf, to ensure: • For all suppliers, that appropriate data processing clauses have been included in the contract. • For suppliers based in countries not covered by 'UK adequacy regulations', that an appropriate mechanism is in place to ensure the lawful transfer of the personal data overseas.	Using a supplier to handle personal data on the University's behalf is known as using a data processor. There are complex compliance rules about the necessary contractual and other provisions when doing this. There is an extra layer of considerations if the supplier is based in a country not covered by UK adequacy regulations. Note that all EU/EEA countries, and a limited range of others, *are* covered by such regulations. The guidance pages explain these rules and contain links to the full list of countries covered by UK adequacy regulations. In short, if you are using standard University terms and templates and/or you contracted via central Procurement Services/UIS, the compliance considerations are covered and no further action is required. If not, the standard terms and conditions of major cloud-based IT suppliers (e.g. those offering services in the areas of data storage, online surveys/forms, mass communications or event management) usually contain adequate clauses. You should focus on any unusual supplier arrangements put in place by the department, and seek advice from the Information Compliance Office if necessary.	
10 Recordings of lectures and other sessions for teaching and learning purposes	If you are a teaching department, consult the latest policy, guidance and templates issued by the Educational Quality and Policy Office on the recording of lectures and other sessions *for teaching and learning purposes*. Review your processes to ensure that your department is collecting consents from teaching staff and students as necessary.	Creating a recording of a lecture or other session (e.g. a seminar) for teaching and learning purposes involves processing the personal data of the lecturer as well as the attendees. The University's policy framework is designed to ensure that consents are collected from those with a core participatory role in any given teaching session (e.g. the lecturer/seminar leader themselves, and students actively participating in small-group teaching sessions). Students just attending a lecture or large seminar simply can be informed that a recording is being made and given	

		an opportunity to 'opt out' from being captured (e.g. by sitting in a particular part of the room or turning off a webcam).	
11 Photos and recordings for publicity purposes	If, as a department, you take photos at/make recordings of events *for publicity purposes*, check that the relevant consent form templates issued by the Legal Services Division are being deployed by event organisers.	Taking photos at, and making recordings of, events for publicity purposes involves processing the personal data of those who are featured. This may include external guests (speakers or otherwise) as well as students, staff and members of the public attending an event. The guidance and template consent forms/signage (under 'Forms and Agreements' on the webpage) ensure that consents are collected as necessary from those who are identifiable from the photos and videos taken at the event. The consent forms also contain various copyright considerations to enable the publication, dissemination and ongoing use of the materials.	
12 Examination data	If you are a teaching department holding examination records, check that you have issued an Examination Data Retention Policy in line with the latest template issued by the General Board's Education Committee.	Policy on the retention of examination records (e.g. submitted scripts/assessed work, raw marks, examiner comments) is devolved to individual Faculty Boards but they are expected to act within the framework set by GBEC. As well as covering pedagogical matters, the framework helps to ensure that personal data is neither unnecessarily retained nor deleted too early. The framework also takes account of best practice requirements from the OIA (e.g. ensuring that adequate 'evidence' has been kept in the case of appeals).	
13 Data protection and project management	(a) If you are running any ongoing departmental projects or initiatives (not including research projects) that will involve the processing of personal data in new ways, ensure that those responsible for running the project are aware of the guidance on data protection by design. (b) Where you think any given project or initiative might pose a high risk to the individuals whose data you are using, seek advice from the Information Compliance Office	Projects and initiatives involving the handling of personal data (about students, staff, applicants, alumni, etc.) in new ways take place all the time at the University. If your department is running one of these, the data protection by design guidance provides some practical tips to ensure that data protection issues are adequately embedded. For some high risk (in data protection terms) projects and initiatives, a full DPIA might be required using the	

	on whether a full Data Protection Impact Assessment is required.	University's template. Advice usually should be sought from the Information Compliance Office before starting one of these. Even if a DPIA is not required, you can use the DPIA template and/or the Information Security Risk Assessment tool issued by UIS to identify, assess and mitigate any data protection and/or information security risks associated with the project or initiative. Different University procedures (including ethical review) are used to assess data protection risks in the context of research projects, so the data protection by design guidance and the DPIA template are not usually of direct relevance to researchers. (Action 1 in this Checklist, whereby Principal Investigators and other researchers should be reminded of the guidance on data protection and academic research, refers instead.)	

Final Checklist sign off by Departmental Administrator (or equivalent)

……..…..…….……Date……..

Final Checklist sign off by Head of Department (or equivalent)

……..……..…….……Date……...

Please submit a completed copy to data.protection@admin.cam.ac.uk by Friday 29 April 2022.