UNIVERSITY OF CAMBRIDGE
Governance and Compliance Division

INFORMATION COMPLIANCE OFFICE

DATA PROTECTION – ANNUAL COMPLIANCE CHECKLIST FOR UNIVERSITY DEPARTMENTS

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.
- Completion of the Checklist is **strongly encouraged at some point during the 2020-21 academic year**. However, it is not mandatory and formal 'returns' are not being requested at this time. This will be kept under review and may change for 2021-22.
- 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 1, issued November 2020

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.

2. Data protection law principally comprises the General Data Protection Regulation and associated UK legislation (including the Data Protection Act 2018). This legislation 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; 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 **strongly encouraged at some point during the 2020-21 academic year**. However, it is not mandatory and formal 'returns' are not being requested at this time. This will be kept under review and may change for 2021-22.

4. Many departments may have more time to work on the actions in the Checklist over the summer months, but others may choose to focus on it at another time of the year. For this reason it is being issued early in the academic year to allow departments to plan and prepare as they see fit.

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 urged to sign off the completion of the Checklist.

Guidance and advice

9. The Checklist refers as appropriate to specific parts of the University's extensive webpages on data protection.

10. Advice may be sought from the Information Compliance Office (data.protection@admin.cam.ac.uk).

Checklist

Topic	Action	Notes	Complete (where applicable)
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: ○ the Data Protection Policy. ○ the Data Protection Quick Guide. ○ the information about how to report personal data breaches. • Highlighting the following specialist guidance for specific types of departmental staff (as applicable): ○ the guidance on academic research and personal data for researchers. ○ the guidance on data protection by design and Data Protection Impact Assessments for IT and/or project staff. ○ 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.	
2 Information Asset Register	(a) Review, and as necessary update, your department's entries on the University's Information Asset Register. (b) Email Principal Investigators in your department to ask them to add any entries for their core research information	The Information Asset Register 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 information security risks. The IAR guidance page should assist with the process of reviewing entries; it also contains practical	

	assets to supplement the department's administrative ones.	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.	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 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 of 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 announcement in a departmental newsletter or welcome session, an item in a departmental new starter induction form, or any other communication method.	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 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.	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, including an extra layer of considerations if the supplier is based outside the EEA. The guidance pages explain these rules.	

<table>
<tr>
<td></td>
<td><ul><li>For suppliers based outside the EEA (i.e. the EU plus Norway, Iceland, and Liechtenstein), that an appropriate mechanism is in place to ensure the lawful transfer of the personal data overseas.</li></ul></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td colspan="4">Final Checklist sign off by Departmental Administrator (or equivalent)
……………………………………………………..…...…………………..……………Date…………………………………..</td>
</tr>
<tr>
<td colspan="4">Final Checklist sign off by Head of Department (or equivalent)
…………………………………………..……………………………..………………..……Date…………………………………...</td>
</tr>
</table>