UNIVERSITY OF CAMBRIDGE
Governance and Compliance Division

**INFORMATION COMPLIANCE OFFICE**

# DATA PROTECTION – ANNUAL COMPLIANCE CHECKLIST FOR UNIVERSITY DEPARTMENTS, 2023-24


**Summary**

- *Purpose:* 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 fourth version of the Checklist, for 2023-24, is substantially similar to previous versions and covers the same topics.
- *Timings:* **Completion of the Checklist is again mandatory in 2023-24. Departments are asked to submit a completed copy to data.protection@admin.cam.ac.uk by Friday 26 July 2024. All departments that are expected to submit a Checklist are being contacted directly**.
- *Practicalities:* 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.
- *Outcomes and reporting:* Each department will receive an assurance rating and feedback on their completed Checklist. In addition, various follow-up activities and reporting procedures will be implemented.
- *Advice:* Advice may be sought from the Information Compliance Office (data.protection@admin.cam.ac.uk).

Version 4, issued April 2024


## 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 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. While all departments have implemented procedures to comply with the law, they need to complete certain ongoing tasks to ensure that data protection compliance remains up-to-date and operationally embedded. This fourth version of the Checklist, for 2023-24, is substantially similar to previous versions and covers the same topics, though some guidance has been updated. It is accordingly anticipated that the tasks required to fulfil the individual actions should be familiar.

3. The Checklist for 2023-24 is personalised to each department. It ends by reproducing the department's feedback given in 2022-23 and inviting comments, where applicable, on the implementation of that feedback. Departments may wish to address this by cross-referring to their substantive responses to the actions for 2023-24.

*Timings*

4. **Completion of the Checklist is again mandatory in 2023-24. Departments are asked to submit a completed copy, signed by the Departmental Administrator (or equivalent), to data.protection@admin.cam.ac.uk by Friday 26 July 2024. All departments that are expected to submit a Checklist are being contacted directly.** (Other units or sub-departments that are not contacted directly may wish to use the Checklist to guide their work in this area and/or to voluntarily submit a completed copy.)

5. It is recognised that some departments might not have been able to complete all the actions by the above deadline. Where necessary, the submitted copy of the Checklist can indicate that certain actions are ongoing and are intended to be completed by the end of the 2023-24 academic year. Any actions marked as ongoing at the point of submission should be accompanied by comments indicating the planned future work and anticipated timescales for completion.

6. 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*

7. 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. If any department temporarily has neither a Departmental Administrator nor a member of staff responsible for data protection matters, they should seek advice from the Information Compliance Office on how best to coordinate the work.

8. The Departmental Administrator (or other member of staff coordinating this work) 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 ultimately 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, communications, office management, student administration, purchasing or project management).

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

9. Departmental Administrators are asked to sign the Checklist before submitting it, and in so doing to indicate that their Head of Department is content for it to be submitted.

*Outcomes and reporting*

10. Following receipt of the completed Checklists, the Information Compliance Office will:

(a) Issue each department with an assurance rating and feedback on its completed Checklist. To this end, departments are asked to supply brief comments on the tasks undertaken (or ongoing) to meet each of the actions as well as completing a check-box response. The feedback given should be implemented by departments thereafter as appropriate.

(b) Carry out 'spot checks' across a sample of departments to verify that actions have been completed as indicated. To this end, guidance is given about the sort of documentation that might be helpful for departments to retain as 'evidence' of completion. Departments do **not** have to submit all of this evidence with their completed Checklist: it would only be requested during a 'spot check'.

(c) Follow up with departments about any actions marked as ongoing at the point of submission to ensure their completion within the anticipated timescales (thereafter, any residual ongoing actions will be escalated as appropriate, for example to the relevant School).

(d) Compile a report on the Checklist exercise for the University's Audit Committee. Individual departments may be identified in this report.

(e) Seek feedback from departments on their experience of the Checklist exercise and use this (together with the completed Checklists) to review and, where necessary, improve the data protection resources provided and to plan this or a similar exercise in future years.

*Guidance and advice*

11. 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.

12. 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.

13. Online briefing sessions about the Checklist, as in previous years, are being held in spring 2024; details of these are being circulated separately.

**Checklist 2023-24**

| Topic | Action | Notes | Response<br>(Select one check-box for each action; not all actions have multiple check-boxes) |
|---|---|---|---|
| 1<br>Training and guidance | Send an email to all departmental staff:<br><br>• Asking staff to check their training records and, if they have not completed the online data protection training course in the past 2 years, to re-complete it.<br><br>• Reminding staff of the top 5 data protection tips. These refer variously to the Data Protection Policy, the Data Protection Quick Guide, and information about how to report personal data breaches and how to recognise data protection rights requests.<br><br>• Highlighting the following specialist guidance for specific types of staff (as applicable):<br><br>  ○ the guidance on academic research and personal data for Principal Investigators and other researchers.<br>  ○ 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.<br><br>A group email will suffice in most cases as individuals should check their own 'training history' by logging into the University Training Booking System (UTBS). However, Departmental Administrators and others with access to departmental UTBS records can check on online training course completions within their department if desired, so as to approach staff on an individual basis. Departments are also encouraged to check or monitor completion rates using these UTBS records.<br><br>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.<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): the email(s) in question.* | ☐ Complete – add comments here on the activities undertaken: |

| | | | |
|---|---|---|---|
| 2<br>Information Asset Register | (a) Review, and as necessary update, your department's entries on the University's Information Asset Register.<br><br>(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. | The Information Asset Register (IAR) has been operational for several years and contains headline details about all information assets in use across the University. Examples of such assets include staff databases, student records or HR files. Users should log into the IAR system (using their normal cam.ac.uk credentials) and check/update the details already recorded about the information assets in use across their department.<br><br>The IAR has two main purposes: (i) it helps to meet a core data protection accountability requirement (known as 'records of processing activities') which means documentation that maps out an organisation's operations that involve the processing of personal data; and (ii) it assists the University in assessing information security risks related to its current information assets.<br><br>IAR entries need to be periodically reviewed to add any new entries, make factual changes to existing ones (e.g. updating an asset's location or purpose), and remove entries about obsolete information assets. 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.<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): an email to colleagues asking them to review IAR entries or a working copy of the downloaded .csv file.* | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Ongoing – add comments here on plans and anticipated timescales for completion: |

| | | | |
|---|---|---|---|
| 3<br>Records management | Use the guidance in the Master Records Retention Schedule to review retention arrangements for records relating to individual former students and members of staff within your department, and dispose of records that no longer need to be retained.<br><br>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, whether paper-based or electronic) to ensure that these are not being retained unnecessarily. Sections 2 and 6 of the Schedule are directly relevant in this regard.<br><br>(For the purpose of this Checklist, marking this action as 'Complete' means that retention arrangements for records relating to individual former students and members of staff have been reviewed, rather than all records on all topics.) | 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.<br><br>Most departments will already have an annual record-keeping review/disposal process and may have a departmental records management or retention plan to assist with this. 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.)<br><br>Records that no longer need to be retained (or transferred to archives for permanent preservation) should be disposed of securely. For paper records, this means shredding them or adding them to confidential waste. For electronic records, this means fully deleting them, and any duplicate copies, from recycle bins and archives (it is recognised that University-/department-wide backups made for disaster recovery purposes may continue to exist for a limited time).<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a departmental records management/retention plan or an email to colleagues asking for the exercise to be carried out.* | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Ongoing – add comments here on plans and anticipated timescales for completion: |

| | | | |
|---|---|---|---|
| 4<br>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.<br><br>(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.<br><br>'Supplementary' privacy notices may be required, for example, when your department has a formal alumni or development function that uses personal data in specific ways that are not highlighted in the core notice for alumni, or where detailed information about all departmental staff is routinely shared with external organisations as part of public policy work in a way that might be unexpected.<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a file note confirming the date on which this action was completed or an email to colleagues asking for it to be carried out.* | ☐ Complete – add comments here on the activities undertaken: |
| 5<br>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. | ☐ Complete – add comments here on the activities undertaken: |

| | | | |
|---|---|---|---|
| | | *You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a link to the privacy policy as published on the departmental website.* | |
| 6<br>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).<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): the local privacy notice(s) in question.* | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |
| 7<br>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.<br><br>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.<br><br>The owners of any mailing lists for which consents are uncertain should seek advice from the Information Compliance Office. | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |

| | | | |
|---|---|---|---|
| | | *You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): the text seeking the original consent and a sample email illustrating the unsubscribe option.* | |
| 8<br>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 process, 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.<br><br>Students and staff can also ask to opt out at any time, but this option does not need to be repeatedly offered to them. (Note that all departmental staff and students can be included in internal listings, directories and intranet pages.)<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a sample induction document or email offering the opt-out opportunity.* | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |
| 9<br>Suppliers handling personal data | Review any *new* arrangements that have been made within the department since the Checklist was last completed that involve third party suppliers handling personal data on your behalf, to ensure:<br><br>• For all suppliers, that appropriate data processing clauses have been included in the contract.<br><br>• For suppliers based in countries not covered by 'UK adequacy regulations', that an appropriate | 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. | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Ongoing – add comments here on plans and anticipated timescales for completion:<br><br>☐ Not applicable – add comments here on why: |

| | | | |
|---|---|---|---|
| | mechanism is in place to ensure the lawful transfer of the personal data overseas. | 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 'locally' by the department, and seek advice from the Information Compliance Office if necessary.<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a file note confirming the date on which this action was completed or an email to colleagues asking for it to be carried out.* | |
| 10<br>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 attending students. 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). | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |

| | | | |
|---|---|---|---|
| | | *You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a sample consent form or an email to teaching colleagues on this topic.* | |
| 11<br>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 (whether in-person, hybrid or virtual). The guidance and template consent forms/signage (under 'Forms and Agreements' on the webpage) ensure that suitable consents are collected from those who are identifiable from the photos and videos taken at the event, whether by standalone forms or by perimeter signage/advance notification of photography and/or filming. The consent forms also contain various copyright considerations to enable the publication, dissemination and ongoing use of the materials.<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): a sample consent form.* | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |
| 12<br>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 (see the 'Guidance on Retention of Examination Data, Records, and Scripts'). | 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 | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Not applicable – add comments here on why: |

| | | | |
|---|---|---|---|
| | | and the OfS (e.g. ensuring that adequate 'evidence' has been kept in the case of appeals).<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): the policy in question.* | |
| 13<br>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 or unusual ways, ensure that those responsible for running the project are aware of the guidance on data protection by design.<br><br>(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 on whether a full Data Protection Impact Assessment is required. | 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. Examples of such projects might include the development of a new 'people' database for the entire department, the setting up of a new online outreach resource aimed at children, or the creation of a new process to manage departmental alumni communications.<br><br>For some high risk (in data protection terms) projects and initiatives, a full DPIA might be required using the University's template. Examples of projects requiring a DPIA might be the implementation of a new departmental database to manage staff sickness absence, or where a 'covert' CCTV system is being considered for deployment following criminal activity outside a departmental building. 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 | ☐ Complete – add comments here on the activities undertaken:<br><br>☐ Ongoing – add comments here on plans and anticipated timescales for completion:<br><br>☐ Not applicable – add comments here on why: |

| | | | |
|---|---|---|---|
| | | and/or information security risks associated with the project or initiative.<br><br>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.)<br><br>*You may wish to retain the following documentation as evidence of having completed this action (this might be required for a spot check): an email to colleagues asking for the guidance to be considered as part of relevant project initiation activities.* | |

**Name of department (or equivalent) and feedback given to the department on its Checklist for 2022-23 (if applicable)**

[Inserted on a department-by-department basis]

**Comments on your department's implementation of the above feedback from 2022-23 (if applicable)**

Comments……

**Final Checklist sign off by Departmental Administrator (or equivalent)**

An electronic signature or typed name is sufficient. Before signing and submitting the Checklist, the Departmental Administrator should check that their Head of Department (or equivalent) is content for it to be submitted.

Signature……Date……..

**Please submit a completed copy to data.protection@admin.cam.ac.uk by Friday 26 July 2024.**