

Checklist for Partnership Data Protection Reviews

Note: This checklist is to support you in completing Appendix C (Information Security & Data Protection) of the Operations Manual.

1 Overview / General

- For international partnerships - has any relevant national data protection or privacy legislation been identified and documented? Have legal services and / or the information management team been consulted?
- Are you confident that relevant flows of personal data have been identified? I.e.:
 - What personal data of Brookes staff, students or affiliates are we sharing with the partner?
 - What personal data is the partner sharing with us?
 - Do any third parties have access to the personal data?
- If the partnership requires regular sharing of large amount of personal data and / or sensitive personal data has the need for a mutual information sharing agreement been considered? Note: the information management team can advise on this

2 Lawfulness of Processing, Fairness and Transparency

- Personal data can only be processed under one or more applicable lawful bases. If students have enrolled status at Brookes then this will typically be “necessary for the performance of a contract”, i.e. Brookes needs the information in order to enrol them, etc. If not we may need to establish an alternative legal basis such as “consent” or “legitimate interests”. Similarly if we are sharing the personal data of Brookes students or staff with a partner then a suitable lawful basis must be identified. In both instances please speak to the Information Management team if this is not clearly defined.
- UK data protection legislation requires all data subjects to be adequately informed of how their data is being used and who it is shared with, usually via a privacy notice. It should be clear which party (Brookes or the partner) will be responsible for issuing the required information (and keeping it up to date), typically this will be the party collecting data directly from students. Brookes has produced a [privacy notice template](#) which may be adapted for use by partners. Note that if a partner is responsible for providing the privacy notice it should be clear that personal data will be shared with Brookes.
- Will personal data be used for direct marketing? If so it may be necessary to gain the explicit consent of data subjects for such use.
- Data subjects have a number of rights under new data protection legislation (esp. The right of access; the right of erasure; and the right to object to processing). It should be clear between both parties who will be responsible for responding to request to exercise these rights, it may be necessary to develop local policies or procedures to facilitate this.

3 Purpose limitation and data minimisation

- Are we only using personal data supplied by partners for the purposes stated in the privacy information provided to the data subjects? It may be necessary to inform partners of how Brookes is using the personal data internally for them to comply with their own data protection requirements
- Are we only sharing relevant personal data with partners?
- Do we have a clear use / purpose for all the data shared with us by partners? If not it may be unlawful to collect and store this data

4 Personal Data Types and Purpose of Processing – Student and Staff

- The different categories of personal data and data subjects need to be identified and documented (i.e. contact information; qualifications; staff; students, etc)
- Have the purposes for which we require personal data to be processed been identified and documented (see also the previous section)?

5 Accuracy of Personal Data

- Is it clear who is responsible for data quality? Is there a need for local policies and procedures to facilitate this?

6 Information Security

Note: This area is highly dependent on how personal data is being collected and shared and whether or not any third parties are involved. Please ask the IT Services Information Management team for guidance as appropriate.

- For personal data of Brookes staff, students or affiliates shared with a partner - We need to ensure that they will provide appropriate technological and organisational security controls. Depending on the volume and sensitivity of personal data this may require external validation (e.g. ISO27001 certification) or the completion of an information security assurance questionnaire.
- For personal data shared with Brookes - we must be able to evidence that we provide adequate security for any personal data we receive.
- The security of any third parties involved will also need to be assessed.

7 Retention of Personal Data

- Have retention periods for all applicable personal data been defined and documented?
- Are local policies and procedures in place to ensure retention schedules are adhered to and that IT assets containing personal data securely disposed of?

8 Accountability

- Have the IT Services Information Management team been informed of:
 - Brookes data shared with partners?
 - Personal data shared with Brookes (especially where students do not have enrolled status)
- If the partnership involves sharing of large volumes of Brookes' personal data or sensitive personal data a privacy impact assessment may need to be conducted. Please contact the Information Management team for guidance.