*Please note that this document has been adopted by teams within central HR for use in recruitment exercises. Departments may wish to adopt a similar approach locally.*

# University HR: terms of use for recruitment data recipients

*Please note that the following applies to any individual involved in the recruitment exercise receiving personal data[[1]](#footnote-1) from University HR, whether they be internal or external to the University.*

By receiving and opening data containing personal information, you accept responsibility for the data and its security, and agree to comply with the General Data Protection Regulation (GDPR) and related UK data protection legislation, and with relevant University policies on data protection and information security.

In particular, you agree to the following:

1. Personal information shall be used only for the purpose for which it was provided.
2. The data shall be kept securely, and appropriate safeguards shall be taken to ensure that it is not lost or disclosed to unauthorised persons. Unauthorised persons in this context refers to those who have no direct involvement in the recruitment process. This applies even where they have an interest in the outcome of the recruitment exercise and may be members of the University. Details of appropriate security measures are set out in the University’s Policy on Data Protection (available at <https://compliance.admin.ox.ac.uk/data-protection-policy> ) and its Information Security Policy (available at <https://www.infosec.ox.ac.uk/guidance-policy>).
3. If the data is downloaded to a mobile device (e.g. laptop, memory stick, tablet, smartphone), the device must be appropriately secured. A mobile device may be used to store the data only if the device is encrypted.
4. If the data file is emailed, or if it is held outside of the central University firewall, then it must be encrypted at all times, e.g. using the software 7-Zip.
5. Rather than use cloud services such as Dropbox to share information with external participants, recruitment information should be shared using file transfer (e.g. Oxfile or SharePoint) with a password provided via separate means.
6. The data shall only be disclosed to a third party, i.e. any person or body other than the original recipient, where the disclosure has been confirmed with the original sender as part of the purpose for which it was originally provided.
7. The data shall be kept only for as long as it is needed to fulfil the purposes of the recruitment activity. Please take steps to delete the data securely six months after the selection activity has concluded. In the case of recruitment resulting in the appointment of a visa holder, your papers will be requested by the appointing HR team within this timeframe.
8. If a breach of data regulations takes place, this should be reported immediately to the original sender (and for University staff, to your designated departmental contact).

For further information on the University’s Policy on Data Protection, as well as its privacy notices, please go to the Data protection policy at <https://compliance.admin.ox.ac.uk/data-protection-policy>.

1. Please note that the Information Commissioner’s Office defines ‘personal data’ under GDPR as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. For further information, please visit the Information Commissioner’s Office website <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/> . [↑](#footnote-ref-1)