Key Data Protection responsibilities for BU Staff

This is an extract from the BU Data Protection Policy, which sets out a summary of the steps which all staff, and others subject to that policy, should take to fulfil their data protection responsibilities. In taking these steps you may require support or advice from others within BU, in particular the Data Protection Officer (dpo@bournemouth.ac.uk), Legal Services (legalservices@bournemouth.ac.uk) or IT Services. You should never hesitate to seek advice if you have any doubts or concerns about the handling of personal data by yourself or others, or technical questions about IT tools or processes.

Some of these steps are less likely to be relevant in practice for those who do not have management or decision-making responsibilities, but it is still important to understand the principles which apply when decisions are made about processing of Personal Data.

- **Mandatory Training:** Undertake BU's mandatory data protection training within the required timescale. (If you are not a staff member this will not automatically apply to you; you will be told if you need to undertake the training).

- **Processing Personal Data:** Be aware of when, where and why Personal Data is being processed and the need to comply with the Data Protection Legislation. Be particularly cautious about processing special category data (previously "sensitive personal data") or recording comments about individuals.

- **Apply "data minimisation"**. Only process the minimum Personal Data necessary for a particular purpose. Apply access controls, security measures, retention policies and (where possible) tools such as encryption and pseudonymisation. For managers: make sure that your team is aware of the controls, measures, policies and tools used within your team. Remember, the fact that you can access or view Personal Data does not necessarily mean that you should do so.

- **Protect Personal Data:** Apply available data security tools and measures to protect Personal Data from unauthorised access or disclosure. This applies to the way in which you store, use and destroy/delete personal data.

- **Data Breach Reporting:** Promptly report any actual, suspected or potential breach of data security or of the Data Protection Policy, including any "near misses".

- **New processing activities:** If you are involved in planning or decisions about new processing activity (i.e. a new use of personal data), as a project team consider carrying out a Privacy Impact Assessment (PIA) and ensure that these questions are asked and answered:

- Do we need to use Personal Data at all?
- Have individuals already been told about this use of their Data?
- Is there a clear legal basis for the processing (i.e. applicable conditions of processing have been identified)?
- What arrangements or controls need to be put in place before you start processing, to ensure data minimisation and data security?

- **Existing processing activities:**
  - Be aware that your handling of Personal Data must be consistent with relevant privacy notices;
  - Be aware of the basis for processing Personal Data, in particular whether it relies on the individuals' consent and the scope of any consent;
  - Follow any established processes or practices within your team regarding when, how and by whom Personal Data should be used, unless you have reason to think that this approach is inappropriate. Managers should ensure that these are identified to staff during induction. Do not depart from standard process without seeking advice.

- **Sharing or transferring Personal Data**: Be cautious. Be clear about the purpose of the sharing and only disclose what is necessary for that purpose. Except in a true emergency:
  - Only share within BU if the recipient needs the Data for a clearly-defined purpose within the uses described in the relevant privacy notice and in accordance with established practice.
  - Only share outside BU if you are following an established process or practice (see above) or after seeking appropriate advice. BU needs to do "due diligence" (appropriate checks) on the recipients of Personal Data to ensure it will be appropriately safeguarded.

- **Data Retention:** Only keep Personal Data where needed for a defined purpose (including any legal and audit requirements) and in accordance with BU or departmental policy – but seek appropriate advice before destroying or deleting materials.

- **Respond promptly** to requests for information or assistance with PIAs, data audits, subject access requests, data breach investigations and other data protection queries or issues.

- **Seek advice about new processing activities or if in any doubt about data protection issues.**

More information about these responsibilities will be set out in the new full BU Data Protection Policy which will be published shortly and the other policies referenced in the appendix to the Policy.

BU is updating or developing the following main privacy notices to ensure compliance with the GDPR requirements on transparency:

- Student Privacy Notice
- Staff Privacy Notice
- Applications, Enquiries and Events Privacy Notice
- Alumni & Fundraising Privacy Notice
- Research Data Privacy Notice

These will be published shortly.