**Data Protection by Design and Default Checklist**

|  |  |
| --- | --- |
| **Date** |  |
| **Author** |  |
| **Team** |  |
| **Activity being reviewed** |  |

GDPR has introduced new mandatory obligations which require the College to ensure data protection is integrated into all activities involving personal data. These are known as ‘data protection by design and default’.

This checklist will assist you in adhering to these new obligations, identify any required actions and act as evidence of your overall compliance.

☐ We consider data protection issues as part of the design and implementation of systems, services, products and business practices. This may involve carrying out a [Data Protection Impact Assessment](http://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/internal/DPIA---NEW-TEMPLATE_FINAL.docx) in line with the College’s [Data Protection Impact Assessment Guidance](http://www.imperial.ac.uk/media/imperial-college/administration-and-support-services/legal-services-office/internal/Data-Privacy-Impact-Assessment-Guidance_FINAL-3-May-2018.docx).

☐ We make data protection an essential component of the core functionality of our processing systems and services.

☐ We anticipate risks and privacy-invasive events before they occur, and take steps to prevent harm to individuals.

☐ We only process the personal data that we need for our purposes(s), and that we only use the data for those purposes.

☐ We ensure that personal data is automatically protected in any IT system, service, product, and/or business practice, so that individuals should not have to take any specific action to protect their privacy.

☐ We provide the identity and contact information of those responsible for data protection both within our organisation and to individuals.

☐ We adopt a ‘plain language’ policy for any public documents so that individuals easily understand what we are doing with their personal data.

☐ We provide individuals with tools so they can determine how we are using their personal data, and whether our policies are being properly enforced.

☐ We offer strong privacy defaults, user-friendly options and controls, and respect user preferences.

☐ We only use data processors that provide sufficient guarantees of their technical and organisational measures for data protection by design.

☐ When we use other systems, services or products in our processing activities, we make sure that we only use those whose designers and manufacturers take data protection issues into account.

☐ We use privacy-enhancing technologies (PETs) to assist us in complying with our data protection by design obligations.

☐ We implement the lowest access settings to ensure persons are able to decide/control their personnel data from the outset