Data Protection Co-Ordinators
Terms of Reference

Introduction

The role of the Data Protection Co-Ordinator (DPC) is an important part of the information governance structure of the College with regards to data protection. The main purpose of the role is to be a local contact in each Department or Division (as is applicable) for more routine data protection queries and guidance. DPCs are also expected to help facilitate the dissemination of data protection communications within their Department or Division (as is applicable).

Each DPC will receive training in data protection compliance and is expected to continue refreshing their knowledge either through self-study or by arranging refresher training with the Data Protection Officer (DPO) and/or Deputy Data Protection Officer (DDPO).

Other documents of relevance to these terms of reference are the College's Information Governance Policy Framework, Data Protection Policy, Information Security Policy and all associated Codes of Practice.

Responsibilities

DPCs will be expected to:

- familiarise themselves with the College's Data Protection Policy, related procedures and resources;
- assist the DPO / DDPO with respect to the development, implementation, monitoring and review of the DPC's Department or Division's (as is applicable) data protection compliance;
- develop an understanding of the relevant Department or Division's (as is applicable) local datasets and how personal data is used and disposed of, as well as where the key compliance risks are;
- handle routine data protection queries within the relevant Department or Division (as is applicable) and escalate non-routine and more challenging queries to the DPO/DDPO;
- report actual or suspected data breach incidents as envisaged in the College's procedures set out here: http://www.imperial.ac.uk/admin-services/legal-servicesoffice/data-protection/data-breaches/ and provide guidance and assistance to colleagues in the relevant Department or Division (as is applicable) who are looking to report actual or suspected data breach incidents;
- give guidance to colleagues within the relevant Department or Division (as is applicable) with respect to data retention and data destruction including liaising, where appropriate, with the Archiving and Central Records Unit to help procure that data retention is in line with the College Retention Schedule and liaising with ICT with respect to the safe disposal of any IT equipment;

- receive Data Privacy Impact Assessments (DPIAs) completed by project leads in the relevant Department or Division (as is applicable) and assist them in determining whether they can sign off on them or whether the DPIAs need to be escalated for approval to the DPO/DDPO and the Compliance and Information Governance Manager in accordance with the College's DPIA procedure set out here: http://www.imperial.ac.uk/admin-services/legal-services-office/data-protection/dataassessments/;

- maintain a database of all completed and approved DPIAs (i.e. including those approved by project leads and those approved by the DPO/DDPO and the Compliance and Information Governance Manager) as required by the College's DPIA procedure set out here: http://www.imperial.ac.uk/admin-services/legal-services-office/dataprotection/data-assessments/;

- disseminate guidance on best practice and other relevant information about data protection compliance within the Department and/or Division (as applicable);

- help the DPO/DDPO identify areas where specific data protection training is advisable and assist the DPO/DDPO in organising appropriate training.

Last revised on February 2020