# Glossary of terms

|  |  |
| --- | --- |
| Data Custodian | This is another appellation for an Information Asset Administrator (IAA) |
| DPA | The Data Protection Act 1998 is the information law that governs the UK. |
| IA | Information Asset, is a definable group of information, stored in any manner which is recognised as 'valuable' to the organisation. The information which comprises an Information Asset, may be just a piece of sensitive research, a folder on shared drive or the information contained within a full database or application. They are not easily replaceable without cost, skill, time, resources or a combination. |
| IAA | Information Asset Administrator is the person dealing with the management of the information used and processed on a day to day basis. For a system for example, it is likely to be the system administrators. For larger assets, it is good practice to have a segregation of duties between an IAO and an IAA. |
| IAO | Information Asset Owners are the people accountable for the information processed. Information Owners are for example the business owners of services, applications, Shared Network Drives, databases and websites where information is created and accessed by many users. Whilst systems may be owned or supported by IT, the information within it is owned by Information Asset Owners. In less complex scenarios information asset owners are the authors of research papers, dissertations, or spreadsheets (this list is not intended to be exhaustive)  |
| IAR | Information Asset Register, this is the central repository and mapping of the information we process at the University, a sort of catalogue. It is not to be confused with a survey of sensitive data or a collection of information; this is a way to manage our information effectively. Whilst it is in the form of Spread sheet, it is planned to be incorporated into a portal / electronic system at a later date in the IG strategy. |
| IG | Information Governance is the discipline of data protection, information laws and information security often driven by the concept of CIA (confidentiality, Integrity and Availability) |
| IGC | (Checklist) The Information Governance Checklist is the combination of the “old” DP checklist and the IT Checklist |
| IGC | (Committee) Information Governance Committee, this is the approving committee which reports to PRC. |
| IGG | Information Governance Guardians, previously known as DPG, Data Protection Guardians, they are the local contact in faculties and directorate within each Guardians Network. |
| IGGN meetings | Information Governance Guardians Network Meetings, which take place quarterly where compliance, risk management, incidents, policies and information security are discussed. |
| IGO | (Office) The new office is the combination of the records management office with the information security manager. It is made of the head of Information Governance, Tony Brown, the deputy head of information Governance, Barbara Frost, the head of data protection (to be recruited) the record manager Alan Carter, the Information Governance Officer, Laurence King and the two Data Protection Officers, Marie Clare and Lisa Crawley.  |
| IGO | (Officer) this is Laurence King assigned to FBMH and the Faculty of Humanities. There is another IGO to be recruited to complete the team. |
| IG Performance Metrics | Information Governance Performance Metrics, often shortened to “metrics”. This is a series of 16 statements with four possible answers, Red, Amber, Green and Blue. Each School / Division / office will be asked to declare their IG maturity. IGGs will be asked to complete this every quarter ahead of the IGC meeting. (Blue is for best practices but we are aiming for good practices, green) |
| IGRR | The Information Governance Risk Review is a tool developed on SharePoint and is a series of questions, which will determine whether your initiative or project is high, medium or low level. You are likely to be asked to complete an IGC, Information Governance Checklist to carry out a full risk assessment and a privacy assessment. Your initiative is likely to be high if you are processing sensitive data, use third party suppliers, includes cloud technology or have to comply with many regulations such as cyber essentials, the NHS IG Toolkit amongst others. |
| IGSC | Information Governance Sub Committee, this is the operational group that reports to the IGC |
| Incident Mgt | Incident Management is the discipline of reporting, investigating, resolving and taking lesson learnt from incidents or data protection breaches. |
| GDPR | General Data Protection Regulations, this is the new European regulations which will replace the Data Protection Act 1998, this will happen regardless of Brexit and we have a duty to be compliant by May 25th 2018. This is one of the big drivers for the new initiatives being introduced at the University such as the Information Asset Register. |
| SIRO | Senior Information Risk Owner, this is the person ultimately accountable for managing risk management for all IAOs and IAAs. The SIRO does this through awareness and championship of the Information Asset Management programme, which includes the Information Asset Register maintenance. Typically, all IAOs should make an annual statement to the SIRO to confirm that their assets are well managed and that there is no major risks identified. If there are risks, it must be accepted, mitigated, transferred or avoided, documented in risk registers for the SIROs scrutiny. Our SIRO at the University is the Director of Finance Steve Dauncey.  |
| 2FA | This two Factor Authentication, when you log on to the University system, it will be a two stage log-on. The first is something you know (your password) and the second one is something you get, it will be an electronic generated pin. Upcoming project but not in the faculty yet. |