**Information Security Classification Scheme – quick reference table (Protective Marking)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Code** | **Classification Type/Name** | **Description** | **Examples** | **Risk Rating** | **Control (Handling)** |
| 1P | Public | Any information published or available publicly. | * Information on the University website including the FOISA MPS and public intranet pages
* Leaflets/booklets
 | Low | **N**ot specified. |
| 2I | Internal | Any information circulated within the University only. | * Internal staff communications
* Information for future publication (FOISA s.26 exemption)
* Timetables/room bookings
* Internal only intranet pages
 | Low/Medium | **I**nternal mail.**E**mail links to files, not attachments where possible. |
| 3R | Restricted | Information which is only accessible to certain employees/groups/committee members/contracted parties. | * Password protected or ‘access restricted’ information (other than personal data)
* Disaggregated statistics e.g. detailed enrolment information
 | MediumDisclosure would risk harm to the University | **I**nternal/external mail, recipient advised.**A**dhere to policy requirements for remote/mobile working. |
| 4C | Confidential | Any personal and confidential information* **Any** personal data under DPA Sch 2 (FOISA s.38 applies).
* Any FOISA exemption applies. Disclosure would **prejudice** the interests of any person and/or organisation.
 | * Student Records
* Staff Records
* CCTV Recordings
* Certain committee & meeting papers/minutes (**Communication Issues section refers**)
 | HighDisclosure of personal data would breach the Date Protection Act & risk action by the ICORisk of harm to individuals and/or the University. | **E**ncrypt external email.**T**racked/’signed for’ mail.**D**ouble envelope **O**ut of view**L**ocked cabinets.**A**dhere to remote/mobile working policy requirements. |
| 5P | Protected | Highly sensitive information * **Sensitive** personal data (DPA Sch 3). Disclosure would be in breach of the Data Protection Act.
* Information which is exempt under FOISA, particularly s.30 (conduct of public affairs) in conjunction with s.33 (commercial interests) and s.36 (confidentiality). Disclosure would **substantially prejudice** the interests of any person and/or organisation and would be actionable by another party.
 | * Disciplinary records
* Any individual’s medical information
* Committee meeting restricted agenda items
* Information related to attempted/actual security breaches
* Certain committee & meeting papers/minutes (**Communication Issues section refers**)
 | HighDisclosure of personal data would constitute a breach of the Date Protection Act and action by the ICO incl possible finesHigh risk of substantial harm to individuals and/or the University | **E**ncrypted email.**T**racked/’signed for’ mail.**D**ouble envelope **O**ut of view**L**ocked cabinets.**M**obile working – no paper, VPN only. |

**Reviewers please note that the Quick Reference Guide will be supported by a fuller document which gives more detail. I have included a few relevant notes below. Please let me know if you have any comments or would like anything included. Thanks. Diana (****D.Watt@napier.ac.uk** **/x 6257)**

**Add to RRS template**

**Notes**

**Code:** Alternative to using Classification Type/Name to mark documents/emails.

**Description:** These have been aligned with information legislation to highlight the types of information which are riskier for the University to process.

**Examples:** More examples will be given in the main document. If you could provide me with examples that you would like to have included that would be useful.

**Risk Rating:** More practical examples of the risks and how/why they occur will be included in the main document e.g. how data loss can occur, examples of how it can be disclosed/distributed in error. Guidance and links to other guidance will be provided e.g. Data Protection Code of Practice, Procedure for a Breach of Data Security, IS Security Policies, Home Working Policy, etc.

**Control (Handling):** Again more detail will be provided in the main guidance document e.g. Out of View = information must be kept out of sight of unauthorised colleagues/persons e.g. PC monitors should not be visible to the members of the public and you should be aware of who may be able to see your screen when working remotely (mobile in a public place, train, bus, etc.) and that it is best to operate a ‘clear desk policy’ as a general rule to minimise the risk of leaving personal, confidential or sensitive information in view on your desk.