Information Classification Scheme

|  |  |
| --- | --- |
| Responsible Office | Governance, Legal & Compliance + IT Services |
| Responsible Officer | University Secretary + Chief Information Officer |
| Approving Authority | Information Governance Group |
| Date of Approval | [2 February 2023] |
| Effective Date | [2 February 2023] |
| Related Procedures | Data Breach Procedure |
| Related University Policies | Data Protection Policy |
| Amended (if applicable) | n/a |
| Supersedes | (New) |
| Next review due | February 2027 |

# Introduction

Bath Spa University aims to embed good information handling processes in all that it does, and endeavours to make protecting information part of its culture.

This Information Classification Scheme provides guidance on the classification and handling of information, and the different levels of security required. It applies to all information held by the University in any format (electronic and hardcopy).

Information should be labelled as Public, Restricted or Confidential by information owners according to the classifications set out below. Unclassified information should normally be treated as confidential.

The scheme will help to:

* protect information from accidental or deliberate compromise, which may lead to damage and/or be a criminal offence
* meet legal, ethical and statutory obligations
* protect the interests of all those who have dealings with the University and about whom it may hold information (including staff, students, alumni, research participants, collaborators, business partners, supporters)
* promote good practice in relation to information handling

# Scheme

|  |  |  |  |
| --- | --- | --- | --- |
| **Classification** | **Public** | **Restricted** | **Confidential** |
| **Information/ Information Asset** | BSU information that can be seen by anyone. | Non-confidential information where dissemination is restricted for policy or contractual reasons, e.g. to members of BSU, a committee, partners, suppliers or affiliates. | Information which is sensitive because it is sensitive personal data, commercial or legal information, under embargo prior to wider release, or which could not be disclosed due to legal restrictions.  Included information about an individual or the institution.  May also include information provided to BSU by other organisations. |
| **Risk** | *Low -* information can be disclosed or disseminated without restriction because it would not breach any relevant laws (notably privacy) or a duty of confidence | *Moderate -*  refers to information that would not be released into the public domain without some sort of risk evaluation, including under privacy laws. | *Serious -* where there is a risk of harm to the University’s reputation or a significant financial impact on the University, its affiliates or a third party. Where either personal (or sensitive personal), internal service configuration or business sensitive data being divulged would equate to the University being at risk of ICO sanctions. |
| **Personal Data**  **As defined by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). (Please see the University’s Data Protection Policy)**  **(See Examples below)** | May contain very minimal personal information, eg name or photograph.  Personal data is processed in accordance with data protection laws, including relating to privacy notices, data security and data sharing. | May contain personal data, including special category personal data.  Personal data is processed in accordance with data protection laws, including relating to privacy notices, data security and data sharing. | May contain personal data, including special category personal data.  Personal data is processed in accordance with data protection laws, including relating to privacy notices, data security and data sharing. |
| **Freedom of Information Act Requests / Environmental Information Requests** | Likely to be disclosed under FOIA/EIR and requester may be directed to information which is already in the public domain. | May be disclosed under FOIA/EIR unless a relevant exemption applies.  Relevant exemptions may include future publication, research information, personal information, confidentiality, legal professional privilege, prejudice to commercial interests. | Likely that an exemption to disclosure would apply under FOIA/EIR, including personal information, prejudice to conduct of public affairs, confidentiality, legal professional privilege, prejudice to commercial interests. |
| **User Devices** | Password protection suggested: locked when not in use | .Access to the document is restricted, either through physical security (eg locked filing cabinet) or through digital means, such as password protection and/or restricted access to view/edit permissions Passwords to be communicated via a separate mechanism when sharing with colleagues. Locked when not in use.  Disk encryption suggested. | Password protection required. Passwords to be communicated via a separate mechanism when sharing with colleagues. Locked when not in use.  Disk encryption required. |
| **Disposal** | Recycling | Irreversible destruction  Use of certified contractor | Irreversible destruction  Use of certified contractor |
| **Retention** | All information must be retained for the legally or contractually required minimum and maximum periods of time set out in local retention requirements. This will vary based on the type of information. | | |
| **Dissemination & Access Controls** | Can be shared via the web without requiring a BSU username and password.  Can be circulated freely subject to applicable laws eg copyright, contract, competition.  May be accessed remotely and via any device without encryption.  No physical security measures required. | Can be shared via the web but the user must provide BSU authentication or otherwise be restricted.  Can be circulated on a need-to-know basis to BSU members and relevant external individuals subject to applicable laws (eg data protection, copyright) and BSU regulations.  May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption.  Physical security of hard copy document should be implemented (eg kept in locked filing cabinets) | Access to confidential data must be strictly controlled by the document owner or by configuration control, with periodic access reviews..  Some types of confidential information may be shared with authorised users via BSU IT facilities, including remote access, subject to BSU authentication. For web access encryption must be used.  Must not be extracted/ downloaded from BSU IT systems and stored on local IT systems.  All devices used to access confidential information must be BSU managed or be encrypted and require a password or PIN to access (eg personal PC, laptop, tablet or phone).  Physical security of hard copy document should be implemented (eg kept in locked filing cabinets) |
| **Exchange & Collaboration** | Can be exchanged via email or file sharing without needing encryption. | Can be exchanged via email without needing encryption.  Can be shared using BSU IT facilities (eg wiki, shared filestore).  Can be printed and circulated via the BSU internal mail service. | The appropriate method for exchanging information must be decided taking into account the nature and volume of the information being exchanged and the impact of inappropriate disclosure.  Must be encrypted and use BSU provided facilities. Other technical protection may be requested as specified in the relevant DPIA.  Information must be marked 'Confidential' and the intended recipients clearly indicated. An optional descriptor, to state the reason for confidentiality, may be used.  Duplicate copies of confidential information must be avoided. Where copies are necessary the protective marking must be carried with the information. Where paper copies are required for sharing, secure delivery methods must be used. |
| EXAMPLES |  |  |  |
| General **Examples** | * Prospectus, programme and course information. * Press releases (not under embargo). * Open content on the BSU website. * Flyers and publicity leaflets. * Published information released under the Freedom of Information Act 2000. | * Some committee minutes. * Some intranet content. * University timetables. * Online directory of contact details. * Learning and teaching materials. * Procurement documents. | * Student personal details. * Staff personal details. * Sensitive data relating to an individual e.g. research participant data. * Some press releases (under embargo). * Some financial transactions. * Some internal reports. * Some commercial contracts. * Some research data. |
| **PERSONAL DATA – As defined by the General Data Protection Regulation 2016 (GDPR) and the Data Protection Act 2018 (DPA 2018). (Please see the University’s Data Protection Policy)**  **Examples (non-exhaustive)** | **Public/ Information Assets may include but are not limited to:**  Anonymised information - information which cannot identify an individual either in isolation or when combined with other information (Article 4, GDPR). (NB Anonymised data may also carry other handling requirements)  Staff Details shared publicly by the University  Information on individuals made public with their consent including on social media sites or departmental websites | **Internal/ Information Assets may include but are not limited to:**  Staff Names  Staff Work Contact Details (including job titles)  Student Names and Email addresses  Academic Staff Qualifications and  Publication Details  ID Number  Online identifier (social media sites)  Location data  Mobile phone number | **Confidential Information/ Information Assets may include but are not limited to**:  Personal data; home address, personal contact details, NI number, age, individual’s image (including CCTV footage)  Staff appointment, promotion or details of personal affairs, employee contract information, wage slips, passports, driving licences, death certificates and non-disclosure agreements.  Student registration and attendance details, exam scripts, marks, comments on student performance, student academic progression, provisional degree classification prior to formal approval and any publication  Sensitive personal data; data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; and the commission or alleged commission by them of any criminal convictions or offence, or any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.  Biometric data e.g. fingerprints, facial recognition.  Financial information relating to individuals e.g. banking information, salary details, indebtedness (student fees)  Grievance/disciplinary proceedings  References for staff or students UCAS forms |
|  | Dates of birth | Individual’s name plus DoB or other personal data; national insurance number (NI), passport details, home address.  Adding additional combinations of data can change the overall classification (sensitivity) of the information.  Increasing the volume can also increase the classification level. For further detail see the procedure for managing and reporting information breaches. |
| **NON-PERSONAL Information**  **Examples**  **(non- exhaustive)** | Anything subject to disclosure under the Freedom of Information Act 2000 (FOIA)  Department and Course details  Marketing or Press Information  Factual and general organisational information for public dissemination including annual reports or accounts  Public events | HR Policies and Guidance | Information relating to supply or procurement of goods/services prior to approved publication  Research Proposals prior to award - Content dependent  ‘Trade’ secrets, intellectual property intended for commercialisation  Research Data which is security-sensitive or has been similarly classified by an external body (e.g. Government, commercial partner with a confidentiality agreement)  Research papers intended to lead to patentable results (If research is on-going and has not been published)  Details of servers and server rooms  Passwords  Exam Papers  Non-Personal Information which is security-sensitive or has been similarly classified by an external body  Commercial Contracts - University and third-party contract/supplier information  Correspondence with Police, Legal Counsel/Legal advice or other information relating to legal action against or by the University  Market sensitive information |

The above scheme may be clarified or amended as required in accordance with business need on the joint agreement of the University Secretary and the Chief Information Officer.