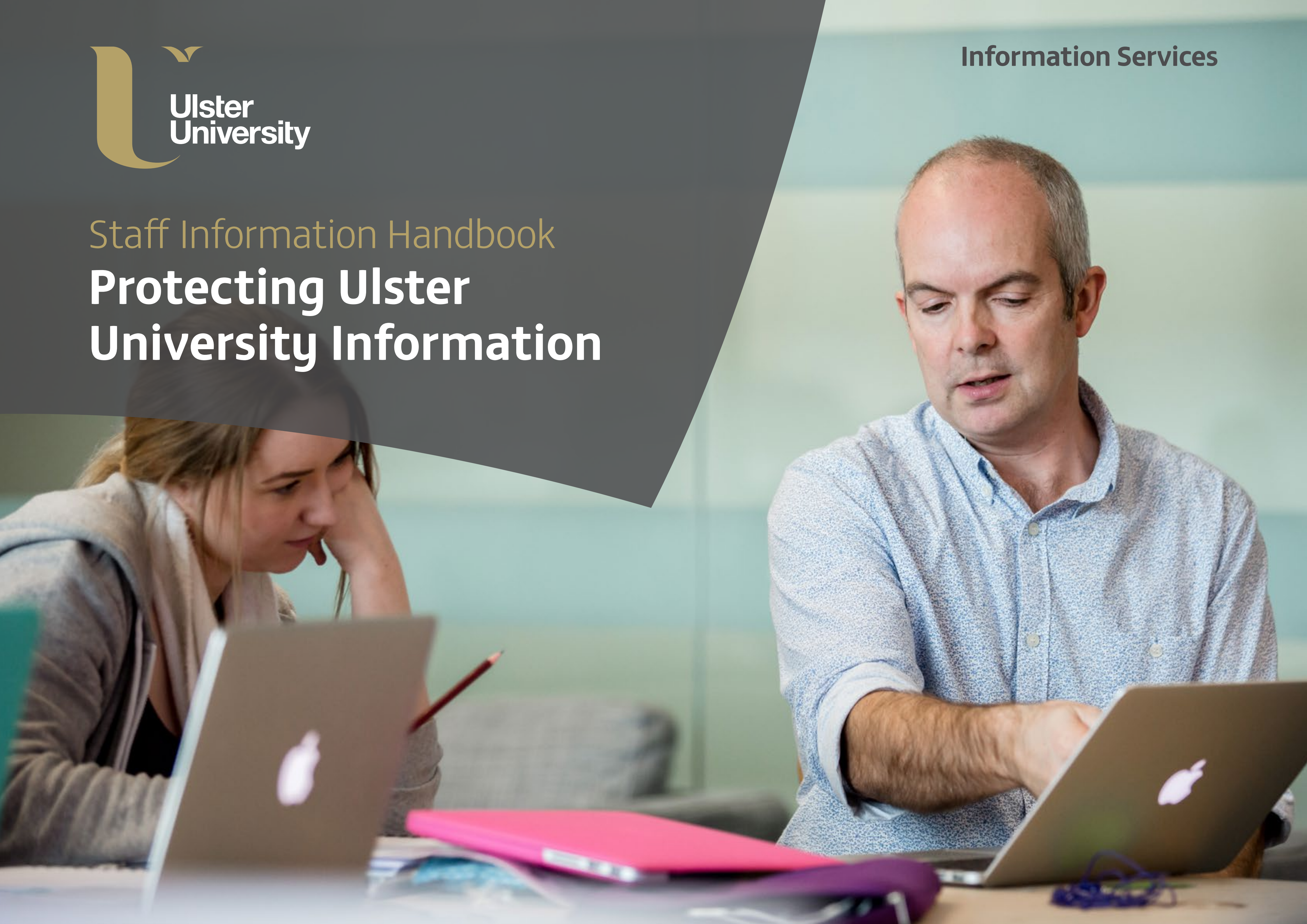
Ulster University

Information Services

Staff Information Handbook

Protecting Ulster University Information



Staff Information Handbook

Protecting Ulster University Information

May 2018

Foreword

Within Ulster University, we have implemented a suite of IT policies, codes of practice, standards and procedures for protecting University information. These are collectively referred to as the IT Policy Implementation Framework, and have been designed to increase information assurance and security along with ensuring legal compliance. An overview of the documents that have been created, approved and reviewed within the IT Policy Implementation Framework may be viewed online at:

ulster.ac.uk/isd/policies/

This Staff Information Handbook distils and presents information assurance and security guidance most commonly required by Ulster University staff in support of their day-to-day tasks.

9 Golden Rules

Working Safely Online – Nine Golden Rules for Staff

1. Protect your password

Never share your password with anyone. No one will ever legitimately ask you to give out your password or PIN number, either over the phone or in an e-mail.

2. Keep your personal data secret

Never give out credit card or other banking details to another person. Do not share personal information such as your address, phone number, family birthdays etc. unless you know or recognize the recipient.

3. Be wary of web links in emails and on web sites

Links could refer you to sites containing harmful viruses or spoof web sites. Check links first or type the address into the address bar in your browser.

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in electronic communications. Communications purporting to be from popular web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting. Be wary!

4. Do not cause offence or break the law

Check out Ulster University's policies and Codes of Practice on Acceptable use of IT Services and Data Protection. Be aware that the University IT systems and networks are monitored for quality, acceptable use and other lawful purposes as defined by the University's Monitoring policy.

5. Secure your personal computer

Lock your terminal when away from your desk; physically secure your laptop.

6. Ensure your business critical data is stored safely

Make full use of on-campus network storage which are regularly backed up, along with your University allocated cloud storage. Ensure you have access to copies of critical data, and do not store sensitive material on unencrypted USB devices.

7. Think about protecting information

Protect personal data of others. We are responsible for managing personal data of others sensitively and securely. Mobile devices are easily lost or stolen. Think before storing personal data or personal data of others on mobile devices. Is the device encrypted?

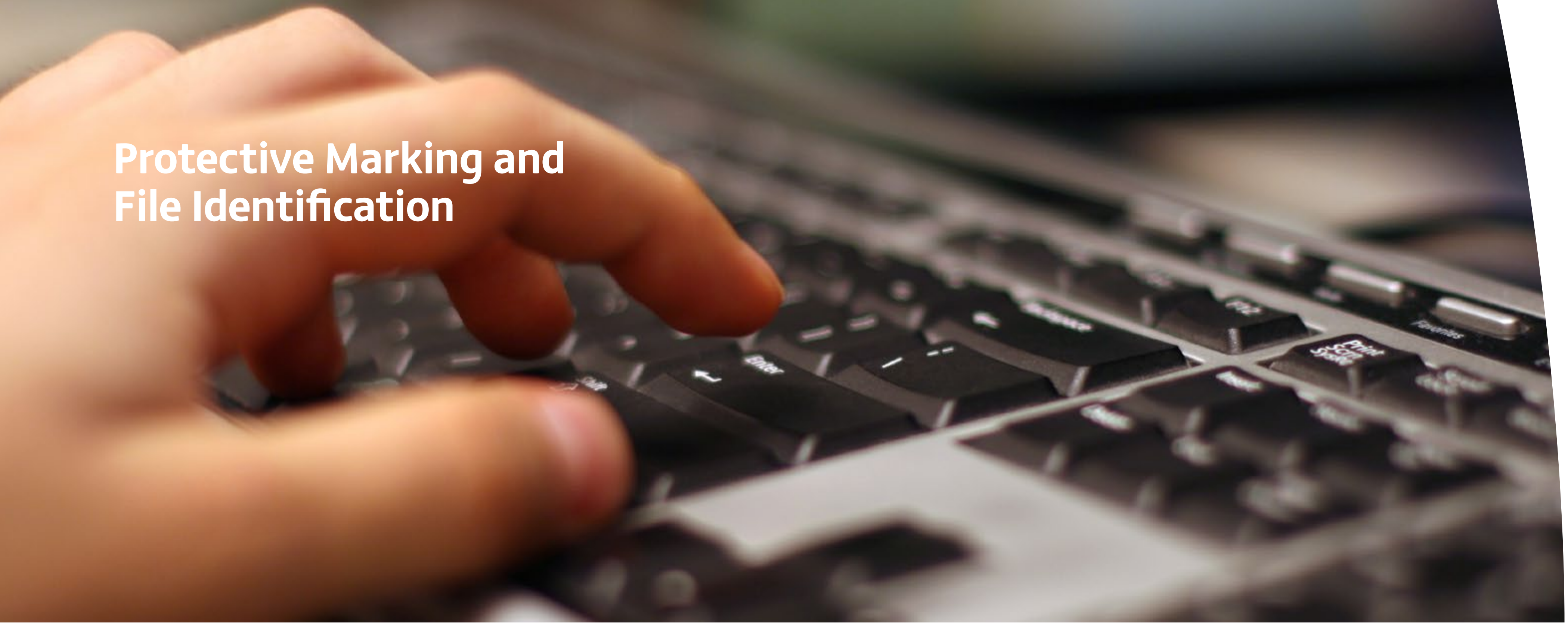
8. Understand copyright

Photocopying and scanning of copyright materials is only permitted under certain circumstances – refer to notices beside each photocopier and visit: **ulster.ac.uk/copyright**

9. Seek advice and assistance

Information Services Service Desk is available on
028 90366777 (ext 66777) or **servicedesk@ulster.ac.uk**
You can also visit the Information Point in the Library on your campus.

Protective Marking and File Identification



A protective marking scheme has been introduced to:

- Help to meet legal, ethical and statutory obligations
- Protect the interests of Ulster University, Staff, Students and the external organisations with whom the University has dealings
- Promote good practice by maintaining reputation, confidence and confidentiality
- Ensure that necessary controls exist to protect the accuracy, completeness and timeliness of the information
- Protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence.

Ulster University has identified information for protective marking including:

- Personal information
- Examination information
- Financial information
- Contract and tendering details
- Sensitive committee business
- Personal information for research projects
- Project specific data.

Protective Marking, Descriptors and Expiry

Ulster University currently has a three-level system for the protective marking of records:

Marking	The Rationale for selection
OPEN	These are documents that do not require classification for the purposes of information security. Unmarked material is considered open or unclassified. The protective marking "OPEN" may also be used to explicitly indicate that this is the case.
PROTECT	These documents if compromised could: • Cause distress to individuals • Breach proper undertakings to maintain the confidence of information provided by third parties • Breach statutory restrictions on the disclosure of information • Cause financial loss, loss of earning potential or could facilitate improper gain or advantage for individuals or companies • Prejudice the investigation or facilitate the commission of crime • Disadvantage the University in commercial or policy negotiations with others.
CONTROL	Additional to those points included in the "PROTECT" classification, these documents, if compromised could: • Cause substantial distress to individuals • Make it more difficult to maintain operational effectiveness • Impede the effective development or operation of University policies • Undermine the proper management of the public sector and its operations.

Protectively marked material shall be marked in UPPERCASE LETTERS, and shall be marked clearly in the document header and footer or where inappropriate to use header & footer, by means of a watermark.

Protectively marked material may also be marked with a descriptor, or privacy marking, which gives descriptive information and/or identifies the reason why the protective marking is applied. The protective marking expiry date (when the protective marking might cease to apply) may also be given.

The descriptor should follow the classification, and be separated by a hyphen (" – "). For example:

- PROTECT – PERSONAL – personal information about living, identifiable individuals.

- PROTECT – PERSONAL – SENSITIVE – As defined by the Data Protection Act 1998: *"the racial or ethnic origin of the data subject, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) whether he is a member of a trade union, his physical or mental health or condition, his sexual life, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings."*

- CONTROL – HR RECORD

- PROTECT – FINANCE

- PROTECT – CLINICAL

Where information needs to be protected for a defined period such as until the commencement of an exam, the document is to be marked as in the example:

PROTECT – EXAMS – EXPIRES 1 JULY 2018 AND BECOMES OPEN

File Names

File names for electronic documents shall be:

- Short
- Clear
- Descriptive
- Specific.

The following are standard elements which shall be considered for inclusion in an electronic document file name of a University Record. When included the stipulated format shall be used:

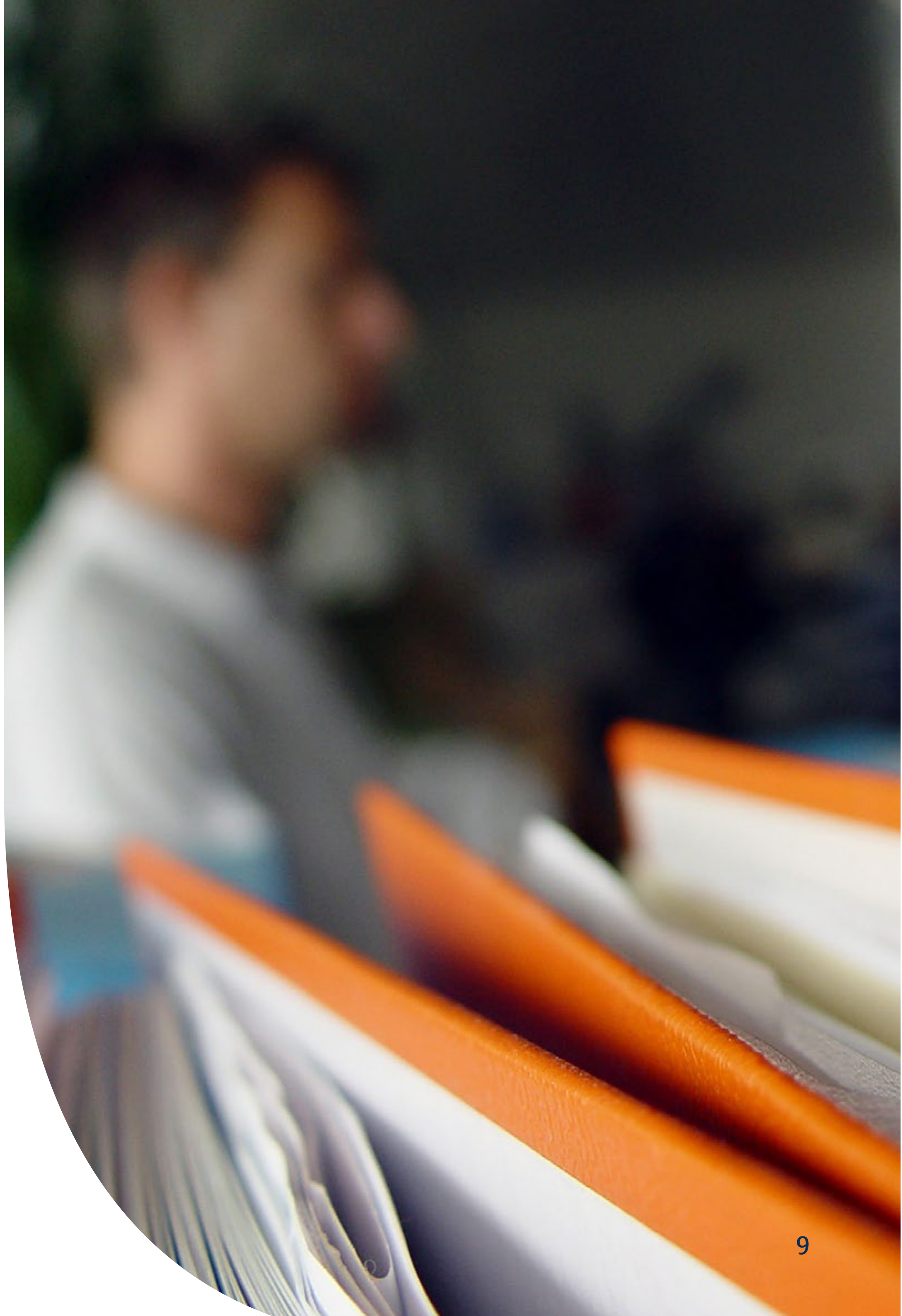
1. Title (No Spaces, Capitalise First Letter of each word to achieve readability);
2. Version ('V' and a number or numbers separated by an underscore e.g V2 or V2_1;
3. Status (Draft, Final, Approved);
4. Protection (Open, Protect, Control);
5. Date (ISO Standard YYYYMMDD or YYYY_MM_DD).

File names shall not contain spaces; Each element shall be separated by an underscore. E.g.

YYYYMMDD_Title_Status_Protection
Title_Status_Protection_YYYYMMDD

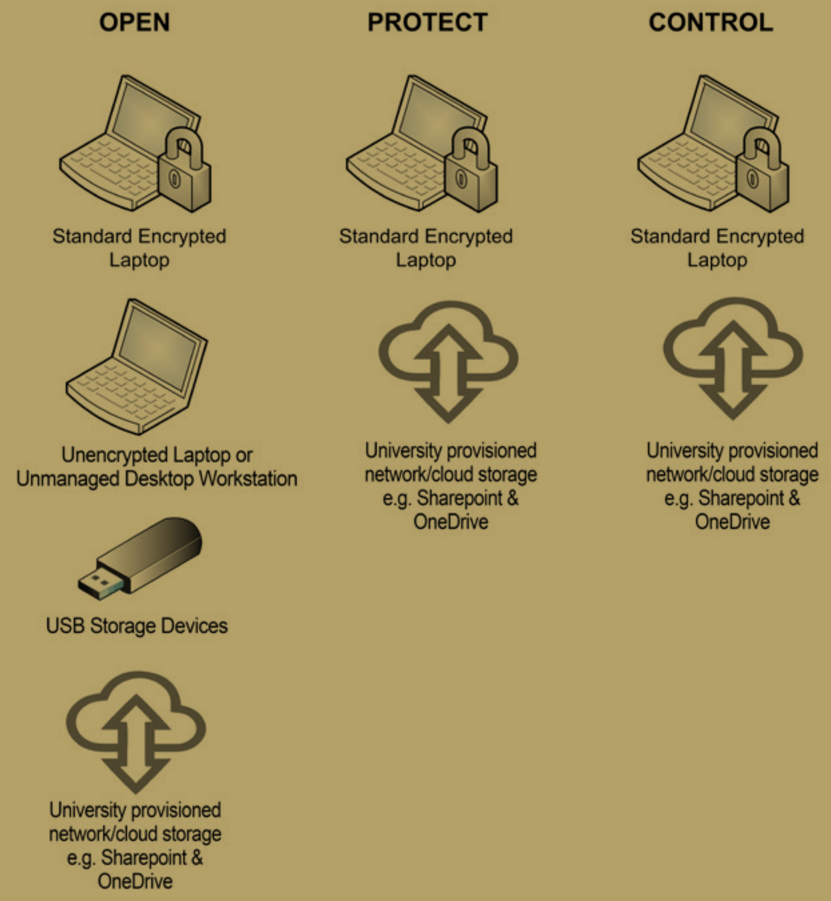
Examples of the above:

1. 20180527_DocumentHandlingCoP_Draft_Protect
2. DocumentHandlingCoP_Draft_Protect_20180421



Storing Information with Protective Marking

Best practice is for electronic information to reside on secure central Ulster University workspace. This helps to ensure that appropriate security and backup measures are in place to protect the information. When it is necessary to store data with Protective Marking on personal workspace, care should be taken to ensure that appropriate security and backup measures are in place. If the storage medium is portable, encryption is required. Staff should only use University provisioned cloud storage such as Sharepoint and Onedrive. Using unapproved cloud services may place information at risk, and can potentially place information outside of U.K. and European legal jurisdictions.



OPEN	PROTECT	CONTROL
Standard Encrypted Laptop	Standard Encrypted Laptop	Standard Encrypted Laptop
Unencrypted Laptop or Unmanaged Desktop Workstation	University provisioned network/cloud storage e.g. Sharepoint & OneDrive	University provisioned network/cloud storage e.g. Sharepoint & OneDrive
USB Storage Devices		
University provisioned network/cloud storage e.g. Sharepoint & OneDrive		

Emailing Data with Protective Marking

Can I email the information...	Appropriate Protective Marking		
	OPEN	PROTECT	CONTROL
To a University email account?	YES	YES	YES
To an external email account?	YES	NO	NO
To my home email account?	YES	NO	NO
To a colleague's home email account?	YES	NO	NO
To my line manager's home email account if asked to do so?	YES	NO	NO

Only OPEN documents may be sent via email for legitimate business purposes.

It is best practice within team sites and file shares to send a path or a link to a document on-line instead of attaching the actual document to an email. Keeping a single authoritative source document helps to avoid confusion over differing versions of documents, increases security control and ensures that periodic backups are conducted.

Removable Media and Portable Devices

The term “removable media” refers to storage media which is designed to be removed from workstations without the need to switch the workstation off. Examples of removable media commonly include:

- USB flash drives and hard disks
- Optical disks (Blu-ray discs, DVDs, CDs)
- Portable music and video players, cameras and voice recorders.

Portable devices commonly include:

- Laptops and netbooks
- Mobile phones
- Pad computers and E-Book readers.

Any portable device that connects to Ulster University network and/or is used to store protectively marked information other than “Open” must employ full disk encryption using approved encryption.

 Optical disks may not be used to store protectively marked information other than “Open”.

Definition of an Ulster University Record

A “record” is information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. These records may be in either electronic or traditional paper format.

Can I place information on...	Appropriate Protective Marking		
	OPEN	PROTECT	CONTROL
My own or third party data stick, laptop or home PC	YES	NO	NO
An optical disk?	YES	NO	NO
A portable device with full disk encryption using approved encryption	YES	YES	YES
University issued encrypted removable media (such as IronKey ®)	YES	YES	YES

Records Retention and Disposal Schedule

Ulster University maintains a Retention and Disposal Schedule to:

- Provide advice to University staff on the length of time records should be kept in Departments or Faculties
- Provide guidance on the legislation applying to particular classes of record
- Ensure that the University can comply with the appropriate legislation.

Further information and links to the schedule are available online at:

ulster.ac.uk/__data/assets/pdf_file/0015/1554/retention-and-disposal-schedule.pdf

Copyright

When staff come across material they would like to reproduce and use they should ask:

- Can I use it under the exceptions allowed for in copyright legislation?
- Or, does the University have a licence to allow me to do what I want to do?
- Or, have I obtained the permission of the rights holder?

If staff cannot answer “Yes” to any of the above, then the material should not be reproduced and/or used. Even storing the material without the rights holder’s permission may constitute copyright infringement. If the material is on a website, look at the Terms of Use on that website.

Further information and links on copyright are available on-line at:

ulster.ac.uk/copyright

Freedom of Information Act

The Freedom of Information Act 2000 (FOIA) gives the public the right of access to information held by public authorities (for the purposes of the FOIA universities are designated as public authorities). Information that Ulster University routinely publishes is available on-line through its Publication Scheme. Other information is made available on request unless there are justifiable reasons for withholding it (known as exemptions). Although University materials will have protective markings and this may help inform decisions to disclose or withhold requested information or to determine the timing of its publication, this will not be the deciding factor to release or not. Only designated officers within the Department of Corporate Planning and Governance are authorised to ultimately determine what information should be made public and what, if any, exemptions might apply.

For further information on FOIA, Ulster University’s Publication Scheme and how to request information visit:

ulster.ac.uk/secretary/policyimplementation/foi.html

General Data Protection Regulation (GDPR)

Note the following GDPR definitions:

“Personal Data” - shall mean any information relating to an identified or identifiable natural person (‘Data Subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological.

“Sensitive Personal Data” - Definition under the GDPR: data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person’s sex life or sexual orientation.

The new 6 GDPR principles set out the main responsibilities for organisations - Article 5 of the GDPR requires that personal data shall be:

1. processed lawfully, fairly and in a transparent manner in relation to individuals;
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

RIGHTS OF DATA SUBJECTS under GDPR

Under the GDPR, an individual has the following rights (all of which rights are qualified in different ways) :

The right to be informed:
The right of access to your Personal Data:
The right to rectification:
The right to be forgotten :
The right to restrict processing :
The right to data portability:
The right to object:
Rights in relation to automated decision making and profiling.

International data transfers

Under GDPR Personal data will only be transferred outside one of the following bases:

- where the transfer is subject to one or more of the “appropriate safeguards” for international transfers prescribed by applicable law (e.g. standard data protection clauses adopted by the European Commission);
- a European Commission decision provides that the country or territory to which the transfer is made ensures an adequate level of protection; or
- there exists another situation where the transfer is permitted under applicable law (e.g. where we have your explicit consent).

ulster.ac.uk/secretary/policyimplementation/dataprotection.html

Further information

If you have any queries on Protecting Ulster University Information please contact:

ISD Service Desk
T: 028 90366777 (ext 66777)
E: servicedesk@ulster.ac.uk

You can also visit the Information Point in the Library on your campus.

Ulster University

Information Services

Designed by: Graphic Design Team (SM), ICTCS