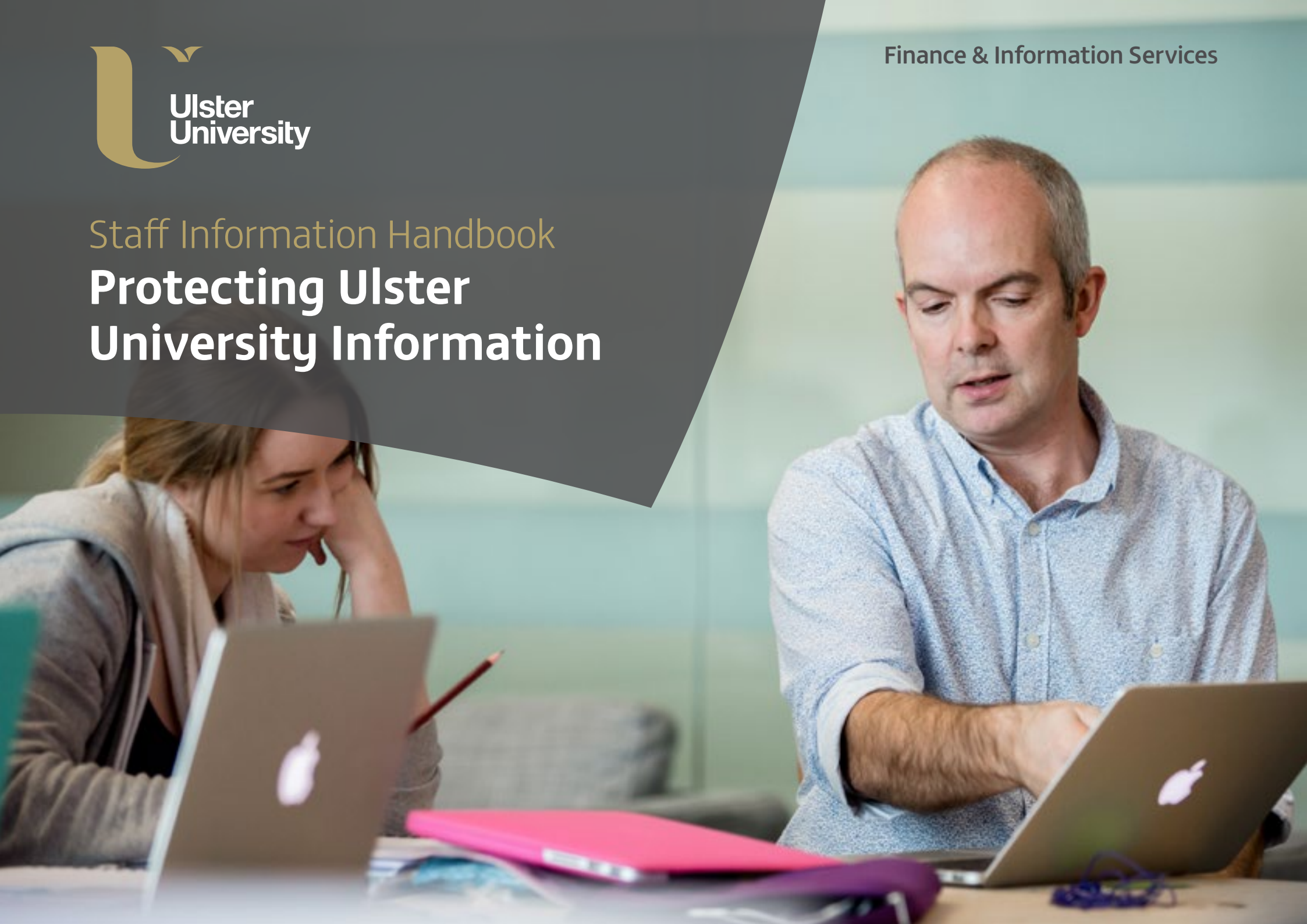
Ulster University

Finance & Information Services

Staff Information Handbook

Protecting Ulster University Information



Staff Information Handbook

Protecting Ulster University Information

October 2017

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/it-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

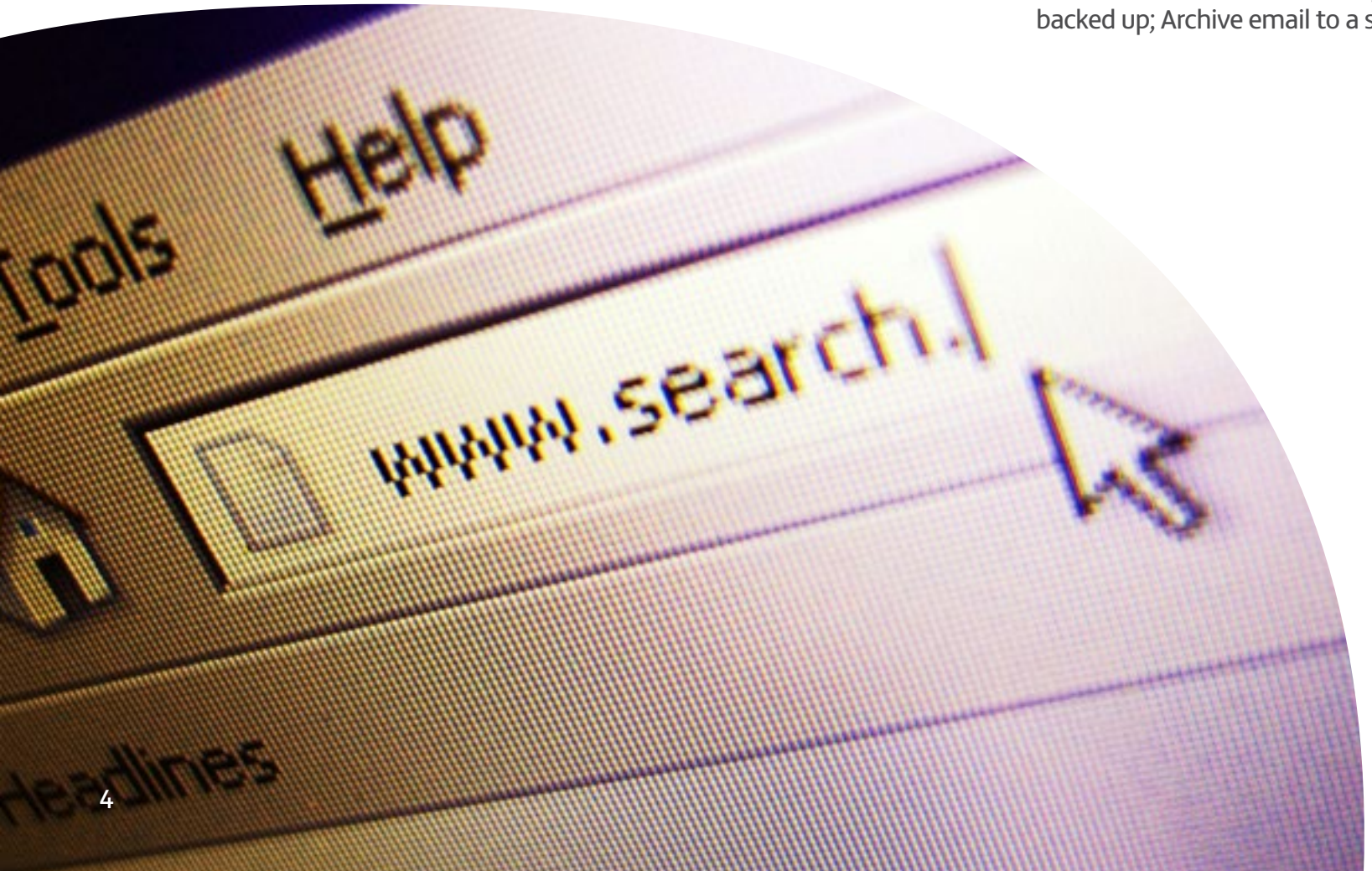
Check out Ulster University's policies and Codes of Practice on Acceptable use of IT Services and Data Protection. Be aware that the University IT systems and networks are monitored for quality, acceptable use and other lawful purposes as defined by the University's Monitoring policy.

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 network storage areas which are regularly backed up; Archive email to a safe store regularly.



7. Think about protecting information

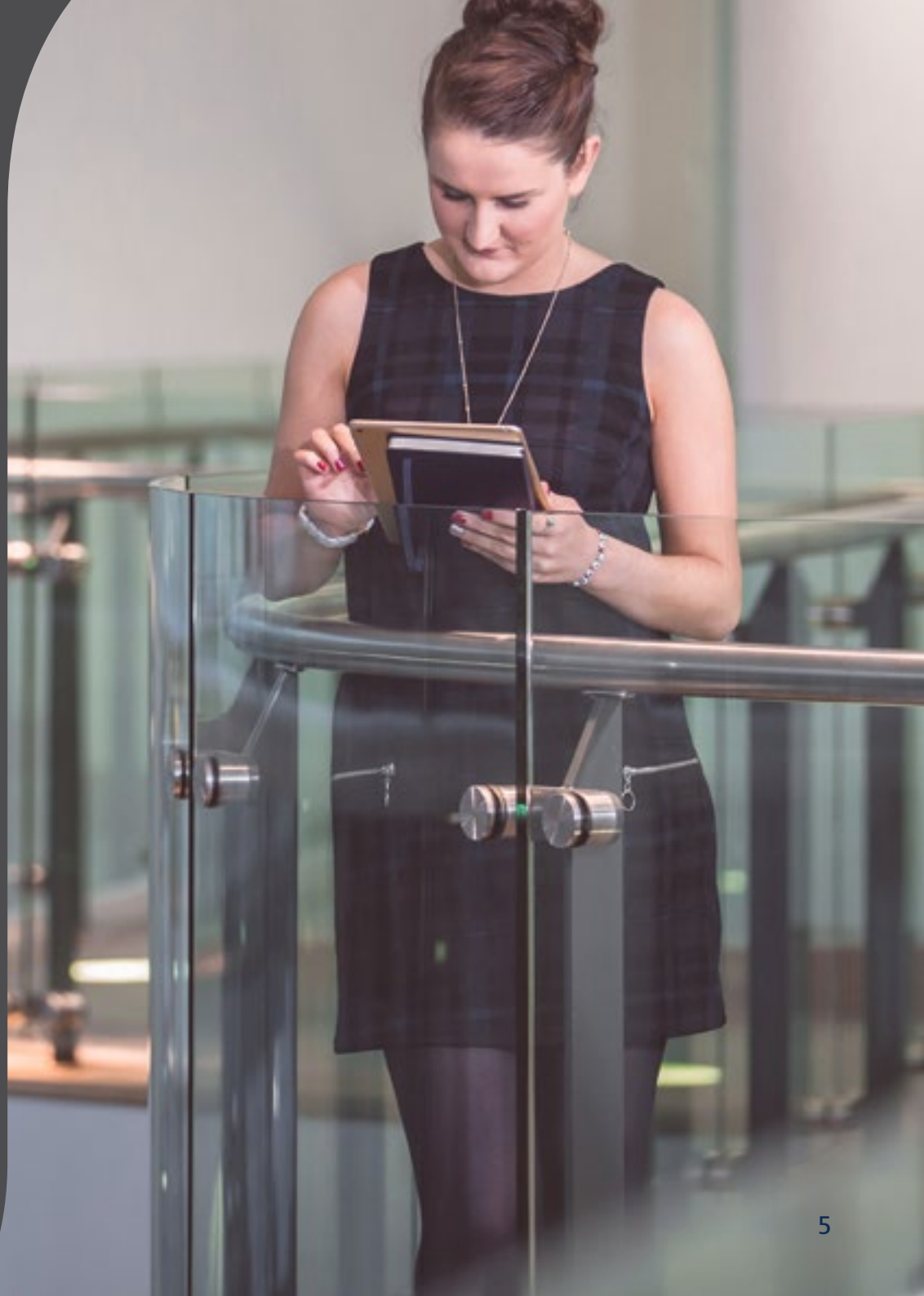
Protect personal data of others. We are responsible for managing personal data of others sensitively and securely. Mobile devices are easily lost or stolen. Think before storing personal data or personal data of others on mobile devices. Is the device encrypted?

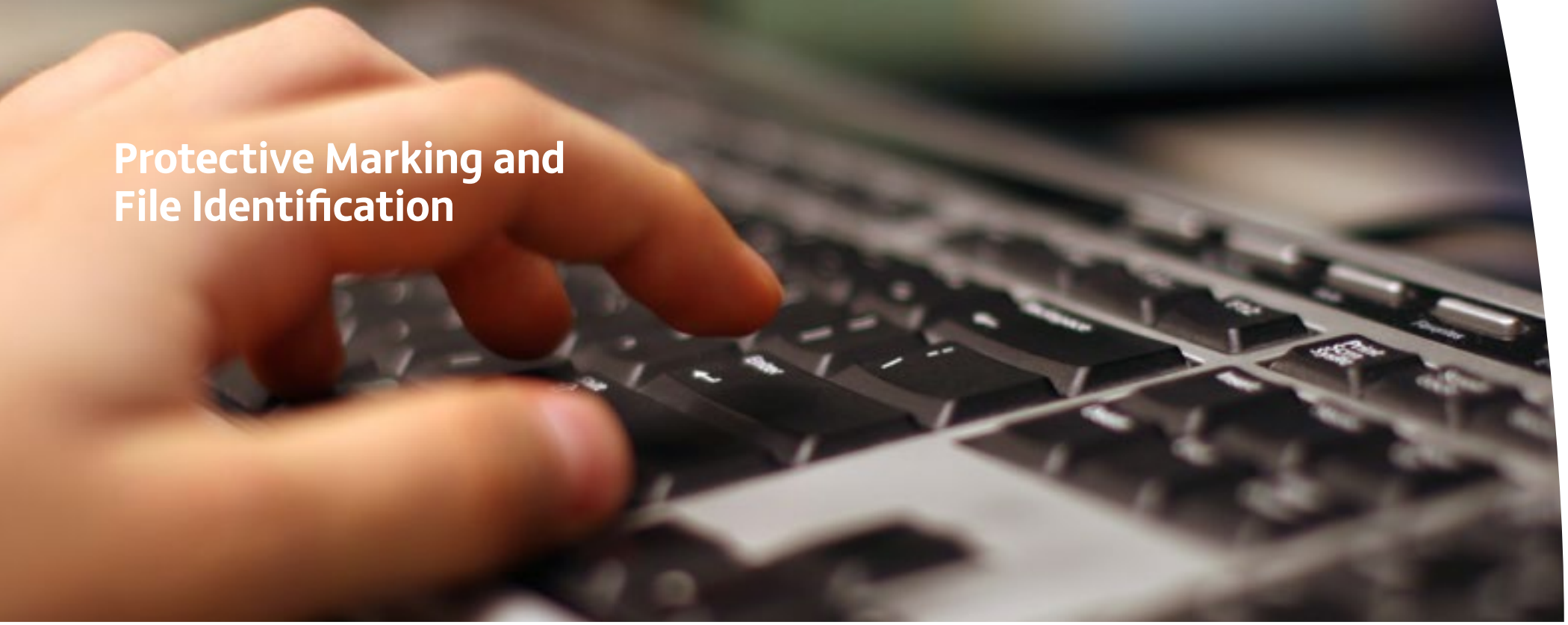
8. Understand copyright

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 11 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:

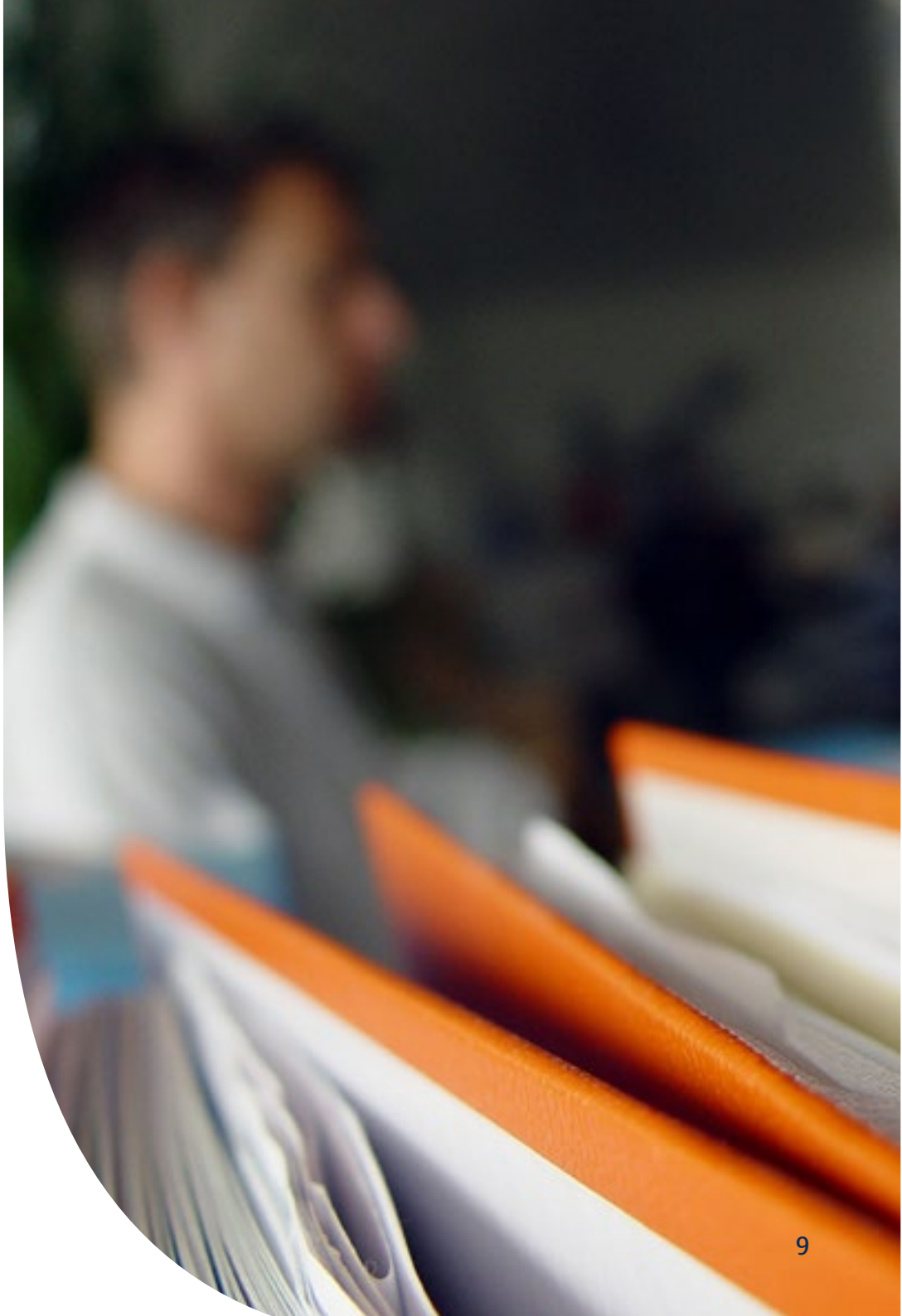
1. Title (No Spaces, Capitalise First Letter of each word to achieve readability);
2. Version ('V' and a number or numbers separated by an underscore e.g V2 or V2_1;
3. Status (Draft, Final, Approved);
4. Protection (Open, Protect, Control);
5. Date (ISO Standard YYYYMMDD or YYYY_MM_DD).

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

YYYYMMDD_Title_Status_Protection
Title_Status_Protection_YYYYMMDD

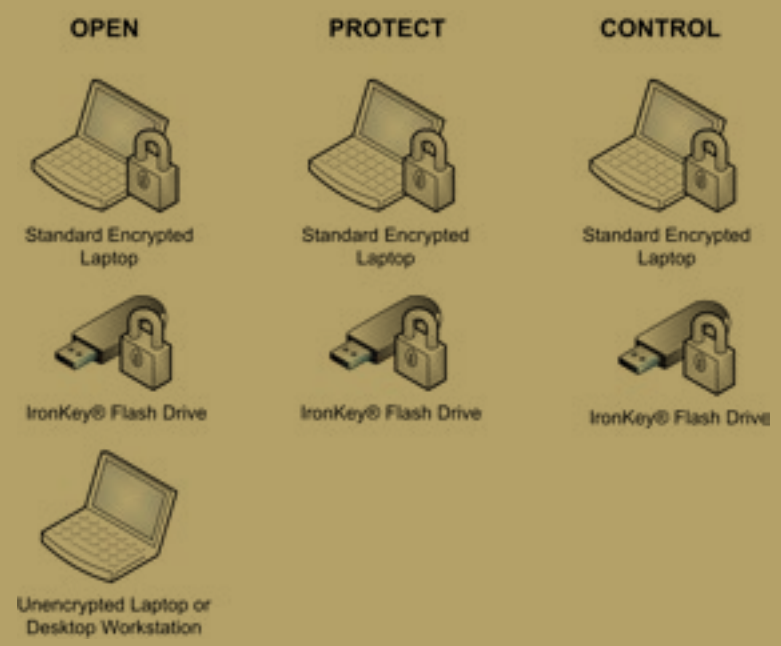
Examples of the above:

1. 20100527_DocumentHandlingCoP_Draft_Protect
2. DocumentHandlingCoP_Draft_Protect_20100421



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 approved external cloud storage. Using unapproved cloud services may place information at risk, and can potentially place information outside of U.K. and European legal jurisdictions.



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)
- Floppy disks or magnetic tapes
- 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.

Only Ulster University issued encrypted removable media may be used to store protectively marked information other than “Open”. 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/0005/92858/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

Data Protection Act

The Data Protection Act 1998 (DPA) is the principal piece of legislation that establishes an individual's rights to have their personal data protected and balances those rights against the legitimate needs of organisations to collect and process personal information for business and other purposes.

The DPA lists eight data protection principles and Ulster University's Data Protection Policy sets out how these apply within the University:

- Personal information must be used legally, fairly and in a way that is open, clear and easy to understand
- Data must be obtained for only one or more specified and lawful purposes and must not be further processed in any manner incompatible with that purpose or purposes
- Data must be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Data must be adequate and where necessary kept up to date
- Personal data must not be kept for longer than is necessary
- Subjects can ask to see what records are held on them. These are known as "subject access requests"
- Data security management, technical and organisational measures must be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA includes a number of exemptions which permit personal data to be either disclosed or withheld if one or more of them can, under special circumstances, be shown to legitimately apply. Although protective markings can be a helpful indicator as to the nature and sensitivity of personal data they will not be the determinant of whether an exemption applies. Only designated officers within the Department of Corporate Planning and Governance are authorised to decide in what circumstances such exemptions can legitimately be applied.

For further information on DPA, the DPA Policy, guidance and training materials, and how to request access to your personal information see:

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

Finance & Information Services

Designed by: Graphic Design Team (SM), ICTCS