



Information Security Policy

This Policy describes how the University manages the data it holds on all staff, students, customers and stakeholders.



Information Security

Policy Statement

This Policy describes how the University manages the data it holds on all staff, students, customers and stakeholders appropriately and with due regard for their confidentiality, integrity and availability.

Currency

This policy is effective from 1 January 2010

Purpose

This information security policy is developed and monitored by Information Technology Services; is owned by the Vice-Chancellor, approved by the Executive, and applies to all data, paper and other media held in the course of meeting the University's mission. The information security policy applies to all electronic and paper based systems hosted either on or off site. Its provisions apply to all staff, students and relevant parties.

Conduct

The University of Derby has legal, ethical and moral obligations to our staff, students, customers and stakeholders in relation to the information held by the University. The University will manage the data we hold on all these parties appropriately with due regard for its confidentiality, integrity and availability.

This policy will be implemented by both University-wide and departmental policies and guidelines.

This policy provides the overarching principles by which information is managed within the University.

The Information Management Co-ordinators Forum comprising appropriate management representation from all areas of the University will devise the detailed policies, procedures, and controls needed to meet the overall policy goal. This group will be steered by appropriate representation within the University's governance structures.

Directors of Service and Deans of Colleges will be responsible for meeting their individual duties regarding the information systems that they operate, though it is expected that most of these duties in the technical areas will fall to the Director of Information Technology Services.

Advice and guidance will be provided throughout the University to all staff, including training and detailed technical advice, where appropriate.

Applicability

It is the responsibility of all employees to do everything reasonable within their power to ensure that the Policy is carried into effect.

Policy Authorisation

Authorised by Head of Governance & IT Portfolio



Freedom of Information Policy

This Policy describes how the University manages Freedom of Information requests it receives.



Freedom of Information

Policy Statement

This Policy describes how the University manages Freedom of Information requests it receives.

Currency

This policy is effective from 23rd January 2013

Purpose

The Freedom of Information Act is intended to allow anyone in the community to obtain information they require from publicly-funded bodies. Hence, the University is covered by the legislation, which places three basic requirements on us:

- That we routinely put in the public domain as much information about ourselves as is reasonably possible
 - That we ensure that, where an individual requires information that we hold but have not already published, we provide the enquirer with the relevant information
 - That we have in place a properly structured approach to managing records to ensure that essential records of our activities are maintained in appropriate detail (and hence relevant information is readily available to the public).
-

Right to request information

The right to request information under the Act extends to anyone who wishes to make an enquiry – they might be an employee or student of the University, an employee of some other organisation or any other member of the public. There is no limitation on who may make an enquiry – the law gives the right to minors and adults alike, and foreign nationals (even those based abroad) are equally entitled to request information.

The University is not allowed to ask enquirers why they require the information they seek. Enquirers need not quote (or even be aware of) their rights under the Act to make a request for information. The only requirement the law places on an enquirer is that they must make their enquiry in writing for it to have the authority of a request made under the terms of the Freedom of Information Act.

Verbal enquiries (e.g. those made over the telephone) do not have the force of law. However, if you receive such an enquiry you should advise the enquirer how to make the request official, and send them the University Request for Information Form and guidance information to assist them in making the request. The Request for Information Form is available to download from http://www.derby.ac.uk/files/foi_request_form.pdf

When an individual makes a written request for information (this includes faxes and emails, as well as letters), the University must provide them with that information, except in a handful of cases where exemptions apply (see Relevant Issues). Hopefully, in most cases this will mean supplying them with instructions about how to find information, using the details provided in the University Publication Scheme. In some cases, however, an enquirer may ask for information that the University does not usually place in the public domain. In these cases, we will have to provide that information directly to them.

The most important thing to remember is that now any letter/email/fax you receive that asks for information may match the definition of a Freedom of Information request and will thus carry the force of the law, and must be responded to in accordance with the law.

To assist you in dealing with the implications of the Freedom of Information Act, one member of staff in your department has been nominated as the Information Coordinator who will take responsibility for dealing with information requests in cases where you cannot personally provide the information requested.

Freedom of Information Policy

Contact details for the Information Coordinators are available at <http://www.derby.ac.uk/foi/contacts>. Should your Information Coordinator be unavailable, contact the FOI Request team on 01332 592151 or foi@derby.ac.uk. In cases where you can answer a request without difficulty then you should continue to do so but a copy of your response must be sent to the FOI team.

In all cases, the information (or ways of finding that information) must be provided within twenty working days of receiving a written enquiry. This is a very short response time so, if you are in any doubt as to whether an enquiry may be a Freedom of Information enquiry, or you cannot respond from the records available to you, please contact your Information Coordinator immediately.

Publication Scheme

The University already places a great deal of information in the public domain, including the minutes from bodies such as the various Teaching and Policy committees, statistics relating to student numbers, the University's accounts etc. These are usually published via the University website though some materials are published on paper and then made generally available (for example the "Welcome to the University" brochure available at Reception points and given out on visit days).

As required by the Freedom of Information Act, all of the information that the University places in the public domain is listed in our Publication Scheme which describes both the types of information available and where it can be located. The Publication scheme information is available at the following URL:

<http://www.derby.ac.uk/foi/publication-scheme>

or downloadable from

http://www.derby.ac.uk/files/foi_publication_scheme.pdf

Handling requests for information

If you are contacted directly by an individual requiring information - either face-to-face, or on the telephone - provide them with a copy of the Request for Information Form and ask them to complete it and return it to foi@derby.ac.uk. Advice and guidance will be provided throughout the University to all staff including training and detailed technical advice, where appropriate.

If you are contacted in writing by an individual requiring information, then you should immediately treat this as a Freedom of Information request. If the information is readily available in your department then you or your departmental officer have to provide a copy of this direct to the enquirer within twenty working days. Alternatively, if the University already publishes the information requested, you or your departmental Information Coordinator has to provide the enquirer with instructions on how to find the information. Usually, it should be enough to direct them to our Publication scheme.

If you receive a request where it is not clear what information is being requested, or where you cannot respond and/or do not know where/if the information can be found, or where the request appears to cover potentially problematic or exempt information (for example, information that might contain the personal details of an employee or student), then you should forward the request to foi@derby.ac.uk or the Service Improvement & Governance Team, E4, Kedleston Road immediately.

NB. If your role involves distributing information on request in any case (e.g. if you are involved in sending out University prospectus) then you should continue to deal with these requests as normal (but please note that the law now strongly requires that you respond within 20 working days).

Relevant issues

(i) Exemptions

The law does permit the University certain exemptions from the usual requirement to respond to information requests. These relate typically to information that may be commercially sensitive and personal information that relates to individuals other than the enquirer. If you receive an information request that covers information that is not in our Publication Scheme and that includes information about individuals (staff, students etc.) or commercially sensitive information, then please pass the request to your Information Co-ordinator immediately.

NB. The Information Coordinator will always take responsibility for refusing any request – refusal should not be undertaken by anyone else.

(ii) Complaints and appeals

In any case where the University declines to respond (or fails to respond fully) to an information request, the enquirer does have the right of appeal to the relevant government body. Should anyone complain in writing to you about the nature and/or content of any response you must forward this complaint to your Information Coordinator immediately.

(iii) Clarification

The University has the right to ask an enquirer for more details to clarify their request in cases where it may not be immediately clear what information they require. If you decide to deal with an enquiry you must be sure that you are clear what information you have been asked to provide: if not, ask your Information Coordinator to approach the enquirer for clarification.

(iv) Costs and fees

The University is permitted to charge fees for any search. The intention of the fee is to cover the costs of the search (i.e. staff time and any copying costs). We do not expect departments to charge for enquiries that can be answered by either the provision of a small amount of documentation (i.e. less than 50 pages) or by giving the enquirer directions to material in the public domain. Any fee charged must be agreed between your Information Coordinator and the University Data Controller.

(v) Statistics

The Act does not require us to provide enquirers with specialist statistical information that the University does not normally produce. Hence, general requests for statistics relating to student numbers can be answered by directions to the Planning and Statistics Unit website: www.derby.ac.uk/statistics. All other statistical requests should be forwarded to the University Data Protection Officer for consideration, though please note that nearly all such enquiries are likely to be refused.

(vi) Organised campaigns

The law allows us to refuse multiple information requests made as part of a campaign. If you receive multiple enquiries of a similar nature you should not refuse to co-operate but you must always inform your Information Coordinator, who will be able to take a view on whether a campaign is being instigated and, if so, inform the University Data Protection Officer.

(vi) Process / Policy validation

This policy provides the overarching principles by which information is managed within the University. An Information Coordinators Forum comprising appropriate management representation from all areas of the University will devise/review the detailed policies, procedures, and controls needed to meet the overall policy goal.

Freedom of Information Policy

Directors of Service and Deans of College's will be responsible for meeting their individual duties regarding the Freedom of Information Act, though it is expected that some of these duties will fall to the Director of Information Technology Services in his role as University Data Controller.

Applicability

It is the responsibility of all employees to do everything reasonable within their power to ensure that the Policy is carried into effect.

Policy Authorisation

Authorised by the Head of Service Improvement & Portfolio



Data Protection Act 1998

Data Protection Act 1998



Data Protection Act 1998

Policy Statement

The University is committed to comply with the Data Protection Act 1998 and will operate procedures to ensure that appropriate requirements are met.

The Act contains eight fundamental principles relating to the collection, use and disclosure of data and the right of staff to have access to personal data concerning themselves.

Currency

This policy is effective from 23rd January 2013

The University and all staff who process or use any personal information must ensure that they follow these principles at all times. Staff should familiarise themselves with the contents of the Data Protection Code of Practice which can be viewed on the University Website.

The University is notified as a Data Controller with the Information Commissioners Office (ICO). This means that the University will notify the ICO of certain details about the processing of personal data which are then included on a public register.

The Director of IT Services has responsibility for ensuring the University's compliance with the Act.

Purpose

Personal data is concerned with data that the University might collect and keep on any individual who might wish to work, works, or have worked at the University. It will include personal details provided in the main from the individual on application forms and other fair and lawful sources.

Conduct

The Principles are that Data will be:

- Obtained and processed fairly and lawfully
- Use will only be for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
- Relevant, adequate and not excessive in relation to the purpose or purposes for which they are processed
- Accurate and where necessary, kept up to date
- Held no longer than is necessary for that purpose or those purposes
- Processed in accordance with the rights of Data Subjects under the Act
- Properly secured against unlawful or unauthorised access, loss, damage or destruction
- Not be transferred outside the European Economic Area unless that country or that territory ensures an adequate level of protection for the rights and freedoms of the data subject in relation to the processing of personal data.

The University will process personal data for the purpose of its normal business activity and in compliance with the law and other statutory obligations. This will include:

Data Protection Act 1998

The payment of salary, pension provision, equality and diversity legislation and the University's duty to monitor statistics, statistical returns, training and development and the operation of policies and procedures. Certain information may need to be disclosed to other legitimate parties as part of the University's obligation to comply with statutory or legal requirements including statistical returns to external bodies including: HESA, Inland Revenue, Pension Bodies and other Government departments, e.g. Child Support Agency and Benefits Agency. These are indicative examples of data processing purposes and are not exhaustive.

The Data Protection Act provides individuals with the right to access to information that is kept about them. Staff wishing to exercise their right under the Act must apply in writing in the first instance to the Data Controller (Director of IT Services).

Applicability

The University and all staff who process or use any personal information.

Policy Authorisation

Authorised by the Head of Governance & IT Portfolio



Data Policy

This Policy describes how the University processes data relating to students.



Student Data Policy

Policy Statement

This Policy describes how the University processes data relating to students.

The University of Derby is notified as a data controller with the Office of the Information Commissioner. The University's Data Protection Officer is Mr. Neil Williams, Director of Information Technology Services. Specific enquiries about student-related data should be made to the Planning & Statistics Unit, Business and Student Support Services (BSSS), in the first instance. All other queries should be made to Neil Williams.

Currency

This policy is effective from 4th April 2011

Purpose

The University processes data relating to its students for a variety of purposes. These include:

1. Management of academic processes (for example, academic audits, assessment of assignments, examination boards, publishing results on notice boards and awarding of degrees)
2. Maintenance of the student record (including personal and academic details)
3. Financial administration
4. The management of university residences
5. Marketing of university courses and services that may be of interest to students
6. Alumni operations, including fund-raising
7. The provision of advice and support to students via, amongst others, BSSS (including Disabilities Services, the Counselling Service and the Careers Service), the Students' Union and personal tutors
8. Internal research, including monitoring quality and performance.

The University, via academic departments, BSSS, and other departments, allows employees and agents of the University to access appropriate information about students, when they have a legitimate reason to do so.

Data Disclosure

Student information is disclosed to a variety of third parties or their agents, notably:

1. Students' sponsors (including LEAs, the Student Loan Company, and funding councils)
 2. University of Derby Students' Union (for membership purposes)
 3. Derbyshire Student Residences Limited (for accommodation purposes)
 4. Relevant government departments to whom we have a statutory obligation to release information (including HEFCE, the Higher Education Statistics Agency, the Department for Education and Council Tax officers)
 5. Examining bodies, other educational establishments and other relevant academic bodies
 6. Potential employers of our students
 7. Potential providers of placements and/or education to our students
-

Data Policy

8. Police (upon presentation of a completed 'Request for Disclosure of Personal Information' form checked by BSSS, or a warrant)

Disclosures will be made to other organisations, not listed above, in specific legitimate circumstances. Consent from the student will be sought where necessary.

Applicability

All staff are directly responsible for implementing the Policy within their business areas.

Policy Authorisation

Authorised by the Head of Governance and Portfolio Office



Data Code of Conduct

Data Code of Conduct Overview



Data Code of Conduct and Procedures

Data Code of Conduct Overview

1. Introduction

Recent years have seen a vast increase in the variety of ways in which data can be created, handled, stored and moved around. People working with data of any sort are in the same position of responsibility that they always have been, and their ethical and moral obligations are unchanged, but it is getting increasingly easy to break that responsibility, be it intentionally or inadvertently.

Handled appropriately, business and personal data are immensely useful and valuable but the consequences of data loss and data misuse are costly, time-consuming, disruptive and unpleasant – the University could suffer significant damage to its reputation and be liable to legal claims and fines from the Information Commissioner's Office. It is therefore committed to managing all data well and to the elimination of data loss and data misuse. All employees are expected to comply with the University's codes of conduct, policies and legislative procedures and to assist in the protection of the organisation. Senior staff are expected to lead by example.

The code of conduct are informed by the University's own Personal Information Promise and Information Security Policy, and by a significant amount of applicable law. The law covers a wide variety of matters including human rights, the investigative powers of police and other bodies, freedom of information, data protection, electronic communications, copyright and defamation.

This document contains the University of Derby data code of conduct, definitions of terms used, the controls to be used when handling data and the reporting procedures for instances of data loss or misuse. It has the following sections:

- A.2. Definition of Terms – to aid understanding of the terminology
- A.3. Policy on Preventive Measures – to outline at top level the policies underpinned by these code of conduct
- B. Data Code of Conduct – the legal framework surrounding personal data, and other obligations that set the rules within which the University must operate
- C. Controls – The behaviours expected of all staff to help the University to ensure that it meets its policies and operates within the code of conduct in Section B. It is important to follow any applicable controls as failure to do so may compromise the University's position or lead to disciplinary action, or both.
- D. Reporting – How to report any potential loss or misuse of data or other breach of the code of conduct.
- E. Maintenance of the Code of Conduct – How the code will be reviewed and kept current.
- F. Audit – Details of how the validity of the code will be monitored.
- G. Examples – Examples of operating both within and outside the code of conduct to help you to view them in practical terms.
- Appendix – Some useful links

Data Code of Conduct

2. Definitions within the code of conduct

Note that within this document “he” and “his” is used as a gender-inclusive substitute for “him or her” and “his or her(s)”

Data - any information at all. This includes, but is not confined to paper documents, images, audio, film or video recordings and files held on computers or portable media.

Data Controller – a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor – any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data Subject – an individual who is the subject of personal data

Data Protection Act 1998 (DPA) – the main UK legislation which governs the handling and protection of information relating to living people.

Freedom of Information Act 2000 (FOI) - UK legislation governing the rights of all people to request information from public bodies (the University is a public body within the scope of this Act)

Personal data – data which relate to a living individual who can be identified –

- a) from those data, or
- b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

It must be noted that payment card data such as debit/credit card numbers constitute personal data and in addition to the legal requirements proper to personal data they also attract very specific and strict contractual obligations. In no circumstances should card payments be accepted without first obtaining specialist advice from the Finance or IT Services departments.

Privacy mark – a label that makes it clear whether something requires handling with particular care for privacy, confidentiality or copyright. Examples could be a page footer marking an entire printed document as confidential and not for reproduction without the originator’s permission, a copyright notice, or a visible label on a CD or USB memory stick.

Processing of data – in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data including –

- a) organisation, adaptation or alteration of the information or data
- b) retrieval, consultation or use of the information or data
- c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- d) alignment, combination, blocking, erasure or destruction of the information or data

Sensitive personal data – personal data consisting of information as to –

- a) 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 (within the meaning of the Trade Union and Labour Relations

Data Code of Conduct

- e) (Consolidation) Act 1992),
- f) his physical or mental health or condition,
- g) his sexual life,
- h) the commission or alleged commission by him of any offence, or
- i) 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.

Staff - any person employed directly or indirectly by the University, or working with one or more University employees on business related to the University's interests.

Subject Access Request (SAR) – the formal means by which any individual can ask to see personal data held on him: this right is outlined in the Data Protection Act

3. Policy on preventive measures

3.1 Expectations of staff

All staff are expected to comply with the University's Code of Conduct. Senior staff are expected to lead by example and display the highest possible standards of behaviour in all their professional activities. Failure to comply with the code may lead to disciplinary action

3.2 Control systems

The University has data management control procedures and standards which employees are expected to follow when conducting University business. These provide compliance with the relevant law and are consistent with best practice.

Details of the Control Systems are given in Section C.

3.3 Reporting instances of data loss / misuse

In the event of any instance of data loss or misuse the University's Information Officer will be notified. All such instances will require corrective action and may provide lessons that inform changes to standard practices in the future.

Details of the reporting measures are given in Section D.

Data Code of Conduct

The code applies to all staff and others working with them on matters in which the University has an interest.

As a public body, the University has a duty when requested by any person to disclose data it holds, unless to do so would be against the law. It is sometimes obliged also to release data that would otherwise be deemed ineligible, in response to appropriate requests from legal bodies such as the police, courts or auditors. All data should be processed, stored and where appropriate catalogued in manners that facilitate this as well as ease of use. It is also sensible to minimise the waste that arises through duplication or holding irrelevant data.

1. Fair & Lawful Processing

All data should be processed in such a way that the University's legal and moral obligations are met.

In particular, personal data shall not be processed unless at least one of the conditions in Schedule 2 of the Data Protection Act 1998 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 of the Data Protection Act 1998 is also met. See section F for links to the relevant parts of the Data Protection Act.

2. Purpose of Information

The purpose for which data are gathered should be clear, legal and consistent with the mission and values of the University. For personal data there is a legal requirement that is significantly stronger:

Data Code of Conduct

Personal data must be obtained only for one or more specified and lawful purposes, and must not be further processed in any manner incompatible with that purpose or those purposes.

3. Data Adequacy

Data should be fit for the purpose for which they are held and processed.

Personal data must be adequate, relevant and not excessive in relation to that purpose.

4. Accurate Information

Data should be accurate and where appropriate kept up to date. In particular, none should defame any individual or organisation.

There is an explicit legal obligation to maintain the accuracy of personal data.

5. Data Retention

Data should not be held for longer than they are needed and where appropriate there should be processes in place for reducing, archiving and deletion.

Personal data processed for any purpose must not be kept for longer than is necessary for that purpose.

6. Legal Rights

All data should be processed and stored in a way that is mindful of the legal rights of those with an interest in them. Copyright and confidentiality must be observed and it should be remembered that under the Freedom of Information Act most of the data we hold are liable for publication on request.

Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act 1998.

7. Information Security

Wherever they may be at the time, all staff handling data are responsible for doing so in an appropriately secure manner and it should be clear what level of security needs to be applied. Privacy marks should be used where appropriate and in cases of doubt the presumption should be in favour of privacy until clarification has been obtained. Data should not be copied unnecessarily onto portable devices or media and when this is done appropriate measures should be taken to prevent inappropriate use, copying, disclosure or loss.

The University and on their behalf, University staff, are legally obliged to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against their accidental loss, destruction or damage.

8. Data Transfers

Care must always be taken when transferring data to ensure their integrity, appropriate levels of security and, when data are passed to third parties, that they have explicit obligations that reflect the code of conduct.

Personal data must not be transferred to a country or territory outside the European Economic Area (EEA) 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.

Controls

This section looks to expand on the University Of Derby Data Code Of Conduct giving clear and concise guidance for all staff. It is however impossible to capture all possible circumstances so when handling data of any sort you should:

- consider the nature of the information, with particular regard to matters such as privacy and copyright;
- consider your actions and whether they are appropriate and
- think about where you are and whether you can be confident of its privacy and that of any system you may be using.

Data Code of Conduct

1. Fair & Lawful Processing

You must

- have legitimate grounds for collecting and using the data; be transparent about how you intend to use the data, and when collecting personal data be able to demonstrate that you have given individuals appropriate privacy notices, and
- handle people's personal data only in ways they would reasonably expect.

You must not

- do anything unlawful with the data either through misuse or illegal copying or deletion
- use the data in ways that have unjustified adverse effects on any third parties

2. Purpose of Information

You must

- have a clear purpose for gathering the data;
- for personal data, be clear from the outset why you are collecting them and what you intend to do with them;
- comply with the Data Protection Act's fair processing requirements, including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Data Protection Act 1998 says about notifying the Information Commissioner and
- ensure that if you wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

You must not

- gather or process data for purposes that are illegal or unfair or
- hold data or process them in ways that are inconsistent with the University's values or good standing.

The retention of data that could support unlawful pornography, harassment, bullying, discrimination or hatred is potentially a criminal matter and will be reported to the

3. Data Adequacy

You must

- hold sufficient data for the purpose for which you are using them.

You must not

- hold more information than you need for that purpose: note that to do so in the case of personal information is unlawful.

4. Accurate Information

You must

- take reasonable steps to ensure the accuracy of any data you obtain;
- ensure that the source of any data is clear;
- carefully consider any challenges to the accuracy of information; and
- consider whether it is necessary to update the information.

You must not

- retain data known to be inaccurate or
- retain data without taking reasonable steps to review and maintain their accuracy.

Note that in the case of personal information these are legal requirements and no information that we hold about any person or organisation should be in any way defamatory.

Data Code of Conduct

5. Data Retention

You must

- review the length of time that you keep data and set an expiry date; ensure that all copies of the data are reviewed; consider the purpose for which you hold information for in deciding whether and for how long to retain them;
- securely delete information that is expired or no longer needed for this purpose, be it by electronic means or by the destruction of paper documents or other physical objects, retaining a record of the deletion/destruction, and
- update, archive or securely delete information as above if it goes out of date while still requiring retention.

You must not

- keep data for which you no longer have a legitimate use or
- make unnecessary copies of data.

In the case of personal information these are legal requirements. Remember also that if the University has to answer a Subject Access Request for personal data or a Freedom of Information request for any other information all copies have to be located, reviewed and possibly provided to the person making the request.

6. Legal Rights

You must

- ensure that all data are marked so that relevant rights (e.g. copyright, commercial confidentiality &c.) are clear;
- assist where necessary in upholding public rights to information held by the University and assist where necessary in upholding individuals' rights under the Data Protection Act.

You must not

- make or store or otherwise handle infringing copies of any copyright material or
- use any material for purposes that infringe others' rights to privacy, confidentiality &c.

7. Information Security

You must

- ensure that all documents (and other objects where appropriate) are clearly marked for privacy or copyright;
- store personal and other privacy-marked information under lock and key or on secure systems;
- control access to any personal or privacy marked information in your possession;
- report losses or suspected losses or breaches as soon as possible, and certainly within 24 hours;
- notify any changes in staff roles to IT Services so that any necessary changes to systems access can be made;
- ensure that data (other than those already in the public domain) on portable systems and media (including laptops, mobile telephones and USB memory devices) are password protected;
- clear all personal or privacy-marked data away when leaving your desk;
- lock your computer and clear the screen when leaving it unattended;
- ensure that when disposing of equipment or furniture any data are securely transferred or destroyed as appropriate;
- be able to demonstrate that you have considered the implications for privacy of any changes to systems or data gathering methods, and
- ensure that any third parties with access to data (e.g. IT support or maintenance companies or business consultants) are bound by contract to adhere to these controls and their staff are aware of their obligations.

You must not

- put personal data on any unencrypted device such as a USB memory stick, DVD, smartphone or portable computer;
- rely solely on document or file password protection to prevent unwelcome disclosure of data;

Data Code of Conduct

- leave privacy marked or personal information unattended on desks, printers, scanners, &c;
- work with personal or other confidential information in situations where it may be overheard or eavesdropped;
- attempt to circumvent any measures put in place to protect personal or business privacy, copyright or the integrity of data;
- interfere with or remove any audit or journaling information gathered while handling or processing data or
- store or process payment card information by any means not explicitly authorised by Finance or IT Services departments.

Note that IT Services monitors and logs computer and communications activities and may use the data gathered either in anonymous, summary form for quality of service and planning purposes or in detailed form following an authorised request to investigate specified misuse, theft, loss, or crime.

8. Data Transfers

In general it is better to place data where those (and only those) with a legitimate right of access to them can all see the same set than it is to make and send copies. If you would like advice on doing this in any specific instances then you should contact IT Services.

When transferring personal data or data that are affected by a need for privacy or confidentiality:

You must

- ensure that the recipient has a legitimate need for the data;
- ensure that you and the recipient have documented his obligation to apply the same controls as are used within the University;
- when transferring eye-readable media ensure that they arrive intact and that the transfer method is auditable (e.g. registered post);
- when transferring electronic media (including USB memory sticks) ensure that they are encrypted and that the decryption key or password is sent to the recipient separately after he has confirmed receipt, and
- when using e-mail use encrypted e-mail and ensure that you and the recipient retain a record of successful sending and receipt.

You must not

- put personal data on unencrypted USB memory sticks;
- put personal data or other data not suitable for publication on smartphones or other portable devices not provided by IT services as suitable for that purpose;
- transfer personal data or other data requiring privacy to any third party without evidence of a clear obligation to observe the University's rules for handling data or
- transfer any data not free for publication to systems hosted outside the EEA

IT Services can offer advice on the use of encrypted media, encrypted e-mail and secure personal devices.

Reporting

If you need advice or are concerned that there may have been a breach of the code you should in the first instance contact your College or Department Information Co-ordinator who may be able to assist. If he is unable to do so quickly or if a breach is confirmed then you should contact IT Services immediately on extension 1234 (01332591234 if you are not on University premises) and confirm by e-mail to ITServiceDesk@derby.ac.uk. Breaches should be confirmed to IT Services within 24 hours.

Data Code of Conduct

Maintenance of the Code







The Information Officer is the guardian of the Data Code of Conduct and responsible for managing the Data Code of Conduct by proposing any major revisions, amendments, or new clauses as appropriate to the University Executive on a periodic basis for approval.

Minor revisions to the Data Code of Conduct for operational reasons, which do not change the authority levels of the Executive or CMT, will be approved using the joint authority of the Vice Chancellor and the University Information Officer whenever they are required for the smooth operation of the University. Any such changes will be updated on the approved Data Code of Conduct provided to staff on the IT Services internal website. The purpose is to make sure the Data Code of Conduct is fully comprehensive and up to date with the policies/procedures, standards and other rules required to maintain efficient management and control of University data.

Audit

The Audit and Risk Committee has responsibility for advising the University Council on the fundamental matter of the effectiveness of management control and the University Risk Management system. The Committee comprises four independent Councillors and is attended by both the Internal Auditors and the External Auditors. The Auditors report regularly to the Committee making recommendations for the improvement of the University's systems of internal control including its Data Code of Conduct. The Committee also considers the management responses and implementation plans.

Examples

-  In April 2009, the University of Manchester e-mailed a spread sheet containing the personal details of 1700+ students and their disabilities to 469 other students.
 -  University of Derby staff will password protect personal data or data that are affected by a need for privacy or confidentiality when transferring to other parties.
 -  In July 2009, Imperial College has six laptops stolen in two thefts. One of the laptops was unencrypted resulting in the information of 6,000 patients being potentially compromised.
 -  If University of Derby staff have a need to transfer personal information they must use encrypted the file or media (USB memory stick, laptop, mobile phone etc.)
 -  A member of academic staff at a university breached Data Protection rules by engaging in correspondence with a parent about her son's studies.
 -  University of Derby staff must not routinely provide information about individuals to third parties, without the consent of the individual in question. If any staff are unsure, or require advice on a topic, they are encouraged to contact <mailto:foi@derby.ac.uk>
-

Data Code of Conduct

Appendix 1

Bibliography

Document Reference	Obtainable from
Data Protection Act	http://www.legislation.gov.uk/ukpga/1998/29
Data Protection Act Schedule 1 – The Principles	http://www.legislation.gov.uk/ukpga/1998/29/schedule/1
Data Protection Act Schedule 2 – Processing personal data	http://www.legislation.gov.uk/ukpga/1998/29/schedule/2
Data Protection Act Schedule 3 – Processing sensitive data	http://www.legislation.gov.uk/ukpga/1998/29/schedule/3
Data Protection Act Part II – Right of access to personal data	http://www.legislation.gov.uk/ukpga/1998/29/part/II
Information co-ordinators – contact details	http://www.derby.ac.uk/foi/contacts
Freedom of Information Act	http://www.legislation.gov.uk/ukpga/2000/36
University of Derby Information Security Policy	https://staff.derby.ac.uk/sites/docs/_layouts/15/WopiFrame.aspx?cedoc=/sites/docs/ppfg/PLCY-Information-Security.docx
Personal Information Promise	https://staff.derby.ac.uk/sites/docs/_layouts/15/WopiFrame.aspx?cedoc=/sites/docs/ppfg/PLCY-Personal-Information-Promise.docx
Payment Card Industry Data Security Standard	https://www.pcisecuritystandards.org/

Responsibilities

Responsibility lies with all University of Derby Staff.

Policy Authorisation

Authorised by Head of Governance and Portfolio Office
