Data Protection Act 1998

Code of Practice

Table of Contents

Introduction

Purpose of this document

If you process personal data about individuals, you have a number of legal obligations to protect that information under the Data Protection Act 1998. This document is intended as a brief guide to the Act and its implications for all members of University of Kent staff.

Further advice can be obtained from Jayne Hornsby, the University Data Protection Officer and the Data Protection team in the Registry datapro@kent.ac.uk

Your responsibility

In dealing with personal data in the course of your employment, you are required to comply with the requirements of the Act.

These requirements are set out in the **eight data protection principles** outlined in this document.

Definitions

The terms and the definitions are derived from the legislation.

Data: means information which:

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
(b) is recorded with the intention that it should be processed by means of such equipment,
(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68, or
(e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

Personal data: means 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.

Sensitive personal data: means 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 (Consolidation) Act 1992),
(e) his physical or mental health or condition,
(f) his sexual life,
(g) the commission or alleged commission by him of any offence, or
(h) 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.

Processing: in relation to information or data, processing 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.

Data subject: means an individual who is the subject of personal data.

Data controller: means 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: in relation to personal data, a data processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Recipient: in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

Third party: in relation to personal data, means any person other than:

(a) the data subject,
(b) the data controller, or
(c) any data processor or other person authorised to process data for the data controller or processor.

The Data Protection Act 1998 Overview

The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect the privacy of their personal details. The legislation itself is complex and, in places, hard to understand. However, it is underpinned by a set of eight straightforward principles. If you make sure you handle personal data in line with the spirit of those principles, then you will go a long way towards ensuring that you comply with the letter of the law[1].

The Act covers information contained in a 'relevant filing system' in a structured format. It is good practice to assume that all manual/paper records of personal data are covered. Manual/paper records must be kept securely.

The Eight Data Protection Principles

The Act requires that the following eight principles should apply to personal data collected, held and stored.

Principle 1:

Personal data shall be processed fairly and lawfully.

In practice, it means that you must:

- have legitimate grounds for collecting and using the personal data,
- not use the data in ways that have unjustified adverse effects on the individuals concerned,
- be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data,
- handle people's personal data only in ways they would reasonably expect,
- make sure you do not do anything unlawful with the data.

Principle 2:

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

In practice, the second data protection principle means that you must:

- be clear from the outset about why you are collecting personal data and what you intend to do with it,
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data,
- comply with what the Act says about notifying the Information Commissioner,
- 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.

Principle 3:

[1] The Guide to Data Protection (Information Commissioners Officer), November 2009

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

In practice, it means you should ensure that:

- you hold personal data about an individual that is sufficient for the purpose you are holding it for in relation to that individual,
- you do not hold more information than you need for that purpose.

So you should identify the minimum amount of personal data you need to properly fulfill your purpose. You should hold that much information, but no more. This is part of the practice known as "data minimisation".

Principle 4:

Personal data shall be accurate and, where necessary, kept up to date.

Although this principle sounds straightforward, the law recognises that it may not be practical to double-check the accuracy of every item of personal data you receive. So the Act makes special provision about the accuracy of information that individuals provide about themselves, or that is obtained from third parties.

To comply with these provisions you should:

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

Principle 5:

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

In practice, it means that you will need to:

- review the length of time you keep personal data,
- consider the purpose or purposes you hold the information for in deciding whether (and for how long) to retain it,
- securely delete information that is no longer needed for this purpose or these purposes,
- update, archive or securely delete information if it goes out of date.

Note: See chapter on retention of personal data.

Principle 6:

Personal data shall be processed in accordance with the rights of data subjects under this Act.

The rights of individuals that principle 6 refers to are:

- a right of access to a copy of the information comprising their personal data (see chapter on subject access requests),
- a right to object to processing that is likely to cause or is causing damage or distress,
- a right to prevent processing for direct marketing,
- a right to object to decisions being taken by automated means,

- a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed,
- a right to claim compensation for damages caused by a breach of the Act.

Principle 7:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

In practice, it means you must have appropriate security to prevent the personal data you hold from being accidentally or deliberately compromised. In particular, you will need to:

- design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach,
- be clear about who in your organisation is responsible for ensuring information security,
- make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff,
- be ready to respond to any breach of security swiftly and effectively.

Principle 8:

Personal data shall 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.

This is the eighth data protection principle, but other principles of the Act will also usually be relevant to sending personal data overseas. For example, the first principle (relating to fair and lawful processing) will in most cases require you to inform individuals about disclosures of their personal data to third parties overseas. The seventh principle (concerning information security) will also be relevant to how the information is sent and the necessity to have contracts in place when using subcontractors abroad.

Responsibilities

Responsibilities of the University of Kent to you as an Employee:

You are entitled to know what information the University holds and processes about you and why. The University must obtain consent from you to process your information, particularly if it is of a sensitive nature. The University must comply with its obligations under the Act. Human Resources (HR) will make arrangements to advise you of the type of personal information held and the reason for any processing of that information on a periodic basis.

Use of the telephone:

You should be aware that the University telephone exchange operates a logging system. The information from the system may be made available to Heads of Sections/Schools.

Use of email:

The University cannot guarantee the security and confidentiality of email. The University maintains logging systems for management purposes, including statistics and for the investigation of possible disciplinary matters.

Your responsibility to University of Kent in relation to:

Your own data:

You should inform HR of any changes to information, which you have previously provided, i.e. changes of address or new information relevant to your employment. HR cannot be held responsible for any errors or omissions unless you have informed them of the changes. You must check that any information provided to you by HR in connection with your employment is accurate and up to date.

The personal data of others:

You must supply information, on request, to the Internal Auditor or the Data Protection Officer relating to all personal data held or used by you in electronic or manual format in connection with your employment by the University.

Controlling Officer:

Staff members controlling personal data should ensure that the following requirements are complied with at ***all times:***

- Any non-standard processing of data must be checked with the Data Protection Officer to ensure that it is covered by the University's description of the processing of personal data.
- All the categories of persons to whom data may be disclosed are included in the University's Registration under the Act.
- Other staff working with the data are familiar with the Act and know what disclosures are permitted.
- The personal data is accurate and kept up to date for the purpose for which it is being used.
- When collecting personal data, the data subject should be made aware of the reason that the data is collected, its use, how long it will be retained and to whom it will be disclosed.

- Data collected and held should be adequate, relevant and not excessive in relation to the purposes for which it has been collected. All data must be deleted or destroyed when no longer required, subject to the retention schedule (see appendices).
- Data is collected fairly and used for the purpose for which it is collected. Additional data must not be collected "in case it might turn out to be useful later on".
- Even if personal data is collected from publicly available sources, e.g. Electoral Roll, Telephone Directory, Who's Who, the use must be registered.
- In the absence for more than a short period of the person controlling the data, information on how to obtain data in response to data subject access enquiries is lodged with the Data Protection Officer or your Line Manager.
- Data is kept securely and cannot be accessed by or disclosed to unauthorised persons. This includes any processing of UKC data off campus.
- Precautions are taken to ensure that personal data is not accidentally lost or destroyed.
- Use of personal data by students complies with the guidance set out below.

Staff supervising Students:

- Advise the student about the requirements of the Act.
- Ensure that students comply with the Act by:
    a) Implementing any instructions issued by you in relation to data
    b) Complying with the General Protection of Data (see page 10)
    c) Consulting with you in any case of doubt over interpretation of the Act and the use of data
    d) Supplying to you the means by which data can be retrieve
- Ensure that the use of personal data is registered – consult with the Data Protection Officer about this.
- Ensure that the data is deleted or destroyed when it is no longer required (see also appendices - Retention of Data).

Other personal data:

If you hold personal data on individuals other than University of Kent staff or students, you must:

a) Advise the data subject of
    - what information you hold
    - what it will be used for
    - what is deemed 'public information'
    - the responsibility of the data subject in supplying correct information and any amendments to such information
    - information on access

b) Obtain the data subject's consent to process.

Specific Guidance for Users

General Protection of Data

The Data Protection Act does not require you to encrypt personal data. However, it does require you to have appropriate security measures in place to guard against unauthorised use or disclosure of the personal data you hold, or its accidental loss or destruction. Encryption might be a part of your information security arrangements – for example, in respect of confidential personal data stored on laptops or portable storage devices. On the other hand, you might not need to encrypt data which always remains on your premises, provided you have sufficient other controls on who can access it and for what purpose. Even where you do encrypt personal data, you will probably need to take additional steps to comply with the Act's information security requirements.

Users must take all reasonable steps to ensure the security of Personal Data and in particular should ensure:

- **Computers** which are used by staff to access personal data should not be placed in public areas where unauthorised persons can read the screens.
- **Personal files** should be kept in locked filing cabinets. Never leave personal information lying on your desk. If possible clear all papers off your desk each evening and file them away or lock them in a desk drawer or cupboard for safekeeping overnight.
- When you leave your **workstation** it is good practice to "lock" it (just hit CTRL-ALT-DEL and click on "lock computer"). This ensures that no one can use your PC while you are away from your desk. It only takes a second or two and keeps information on your PC secure.
- **USB sticks**, other media and printed data should be locked away when not in use and not left in public areas.
- **Unwanted material** should be shredded and placed in a secure waste bag. Arrangements for the collection and shredding of secure material should be made with Estates Maintenance.
- Where practicable, and particularly with highly **sensitive material**, data should be de-personalised or coded in some way.
- Computer **passwords** should not be easily deduced and should be changed regularly. For further information on password security visit Information Services website https://www.kent.ac.uk/itaccount/password/
- **Permissions to systems, folders etc.** are properly set to prevent unauthorised access and are updated when staffs move onto to different schools and roles.
- When data on **CDs and removable hardware** are no longer required, it should be completely overwritten or erased.
- Where data is downloaded from the **Student Data System** to computers, it should not be copied and used elsewhere and must not be kept longer than necessary. Data from this source must not be used to satisfy access requests since it is copy and may be out of date.
- Avoid taking personal information home with you. If you need to save personal data onto a laptop or removable storage (e.g. memory stick) then ensure it is encrypted.

The use of personal mobile devices

With the recent developments in smart phone technology and mobile devices such as i-pads and Notebooks, more University of Kent employees are opting to access emails and connect to the University network remotely.

Working from a nearby coffee shop may seem like a nice idea, but using its Wi-Fi hotspot or any other open public network may jeopardise sensitive data. You should always access business systems through a virtual private network (VPN), which provides a security enhanced exchange of information between remote employees and The University of Kent network.

The home VPN service allows you to access networked resources such as files on the Kent network, e.g. files on the Bodiam or Gromit servers. It is vital therefore that you do not save any personal data onto your home computer and you ensure that no-one else in your household is able to access any information. Also, before applying for use of the VPN Service you must have **up-to-date anti-virus software** installed and ensure you **apply all security updates** to your computer operating system.

In order to apply for VPN access please visit the Information Services website:
http://www.kent.ac.uk/itservices/home/index.html

Where possible, please try to avoid accessing work emails on your personal device as you should have no real reason to do this. If you travel regularly then you may find it beneficial to request a business phone that can be set up correctly with the appropriate security enhancements.

If you do access your work emails via your smartphone then you need to ensure your device is configured properly. The ability to read and respond to work email almost anywhere is one of a smartphone's key benefits. How the phone is configured to access the University of Kent server depends on the model. You may need to install PC-synchronization software in order to link to your email, contact lists and calendars. The University offers support for staff configuring their smartphones for work use, please contact mobiledevicesupport@kent.ac.uk

If you choose to use your personal device for work then you must ensure that your device is password protected with a strong password including upper and lower case characters along with at least one number. Passwords should be reset every 30 or 60 days. Your phone should be set to "time out" after a short period of inactivity, so it will be harder to access if it falls into the wrong hands. Consider encrypting the data on your mobile device through the built-in operating system or third-party software. Your service provider may also be able to lock a lost or stolen device remotely or wipe the data from it. In addition to this you should always remember to lock your device when it is not in use.

Like any other computing device, smartphones are susceptible to technical failure. Because of their smaller size, they're also more likely to be lost, stolen or broken. Synchronization software enables you to back up business-critical data simply by connecting your mobile device to your office computer.

Ensuring that all smartphone applications are up-to-date can also help protect your mobile devices from malware and viruses that target vulnerabilities in their operating systems or browsers. Many smartphones can be set so users are notified by email when new software is available.

Generally, the same rules that are applied to working at your PC should be applied your mobile device so avoid opening suspicious emails, attachments or applications, and don't open links on dubious web pages.

Please note that connecting your personal computer and/or mobile device to the University of Kent network is entirely at your own risk. The University will not be liable for any loss, damage or inconvenience arising directly or indirectly to a personal computer and/or mobile device as a result of its connection to the network. Although the University takes reasonable care to prevent the corruption of information, the University does not give any warranty or understanding to the user about the integrity of information.

The University accepts no responsibility for the malfunctioning of a personal computer and/or mobile device, its hardware or software as a result of its connection to the University of Kent network.

The University accepts no responsibility for the loss of any data or the failure of any security or privacy mechanism on a personal computer and/or mobile device that has been connected or is connected to the University of Kent network.

For more information please see the ***University's Regulations for the use of Computers and Mobile Devices not Owned and or managed by the University and Connected to the University of Kent Network.***

http://www.kent.ac.uk/is/regulations/it/regulations-computers-mobile-devices.pdf

Email Security

- Consider whether the content of the email should be encrypted or password protected. Information Services should be able to assist you with encryption. ***Note:*** If you do encrypt any emails, you will need to be confident that you can access them if asked to produce them for a subject access request.
- It's also a good idea to turn off the **"suggest names" facility** on Outlook. This means you have to type in the address in full or look it up in the address book. It's a small price to pay to avoid those awkward moments when you realise that you've just sent an e-mail to the wrong person.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

Viruses and Spyware

- Make sure that your operating system is set up to receive **automatic updates**.
- Protect your computer by downloading the **latest patches or security updates**, which should cover vulnerabilities.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, and then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update.

Note: *staff managed desktops will take care of security issues automatically. If you are unsure as to how your desktop is managed, please contact* ***helpdesk@kent.ac.uk****.*

Disclosure of Data to Third Parties

The Data Protection Act protects the data subject from unauthorised third parties.

Unauthorised third parties include:

- A person or organisation to whom the data subject has not consented that the data be disclosed,
- A person or organisation to whom the data subject has consented that the data be disclosed, but where the request is for reasons other than that for which the data was collected, or for which the consent was given.

Unauthorised third parties will include family members, friends, local authorities, government bodies and the police, unless non-disclosure is exempted by the 1998 Act, or by other legislation.

Parents and relatives

The general rule is that students and staff are private individuals and the University has no responsibility or obligation to keep their relatives informed of any aspect of their studies, professional activities, or private lives. Therefore when a parent insists that University staff provide them with information relating to their son/daughter then you are able to say that under the Data Protection Act you are not allowed to give out any information about any of our students.

Immigration officials

The University often receives requests from immigration officials about individuals either studying at or on their way to the University. Please pass all these enquiries on to the Student Records and Examinations Office in student_records@kent.ac.uk in the Registry.

The police and other officials

Occasionally, the University receives requests from the police and officials for personal information. It's not compulsory to give out information in these cases. The police can submit a "section 29" form explaining exactly why they need the information. This still doesn't mean that information has to be released, although obviously the University will always try to help where possible. If we still do not want to release the information then the police can force us to do so with a court order. If you receive a request from the police, you should **always** refer this request to the Student Records and Examinations Office student_records@kent.ac.uk

"Other officials" includes benefit fraud agencies trying to confirm that claimants are students and entitled to make claims, or immigration officials checking that a person is a student sponsored by the University. In all these cases it is best to speak to Student Records and Examinations Office student_records@kent.ac.uk

Qualification checks

Employers, recruitment agencies, other HE institutions, and other similar bodies regularly ask for information about our students. Normally they are asking for us to confirm qualifications or provide references so that they can consider a student for a job or a place on a course.

You should always check that the enquirer is who they say they are. If the caller is on the telephone then you could do this by asking them for the main switchboard number of their organisation and phoning them back. You could ask them to e-mail their request or fax it on headed paper. Some recruitment forms will have a sheet signed by the student allowing the recruitment agency to ask for information about them. Sometimes a quick internet check will reveal that the organisation is genuine and that the phone or fax number you've been given is correct. If you aren't certain that the person is who they say they are then ask them to provide more proof, or contact the Data Protection Officer. If you are not comfortable with giving out the information you are being asked for then don't. Generally, you should not need to give the enquirer more than the dates when the student studied here and their marks or degree class.

Occasionally you will be asked to confirm qualifications that someone has claimed to have, but do not actually hold. If the person never studied at the University then we can tell the enquirer that. Because the person was never here we hold no information about them and so the Act doesn't apply.

More information about references can be found on ***Page 22 (see appendices).***

Sharing Information with Colleagues

The University is a single "Data Controller", so passing information about staff or students between staff, schools or sections doesn't include a "third party". However, this does not mean that information can be shared freely. There should be a good reason for the information to be shared, and the minimum amount of information should be shared each time. So it's possible that someone in Payroll needs to know that a member of staff is going to be off sick for seven weeks so that they can make sure they are paid appropriately, but they don't need to know why the person has to take that amount of sick leave. It is particularly important to

make sure that information about sensitive issues, including disability, sexuality or ethnicity is not shared unless it is absolutely necessary.

If you pass information through e-mail or internal post you need to make sure that it will safely reach the person you mean to send it to, and won't accidentally be seen by anyone else. This means checking the name in the e-mail "to" box carefully before hitting "send" or writing the name and department clearly on an envelope. Envelopes and e-mails should be marked "confidential". You should avoid faxing personal information as this isn't secure or confidential.

Transfer of Data outside of the EU

Personal data shall not be transferred to a country or territory outside the EU or 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.

If the University enters into partnerships with overseas institutions it may have to provide details about staff, students or Alumni to that institution. This is permitted under the act only if the country has its own protections which are of a similar standard to the European ones. Please consult the Data Protection Officer who will seek guidance from the Information Commissioners Office.

Please note that the Information Commissioners Office have released a Code of Practice on Data Sharing: https://www.ico.gov.uk/tools_and_resources/request_publications.aspx

Examination Marks

Students have the right to see preliminary marks and comments that contribute to final assessments, if they ask to see them. If a student submits a Subject Access Request (see page 24), the University has to provide access to all examination marks either within five months of the request (if the results haven't yet been published) or forty days after the official release of results - whichever is sooner. The delay is to stop students trying to find out what their marks are before the results are made official.

Release of Exam Marks to Debtors

If a student remains in debt to the University at the time when his/her result would usually be available, the student will be excluded from any pass list, no transcript will be released, the degree will not be conferred and no personal reference is to be supplied.

Should a student make a Subject Access Request for information concerning results, the University will provide the information as required by the Act but will annotate the information to the effect that the degree has not been conferred; the information statement is not a formal transcript; that the student at the time of the access request was indebted to the University; that the information has been supplied in response to an access request under the Data Protection Act.

Examination Pass Lists

You should not post personal information on notice boards. However, the Information Commissioner has said that because exam pass lists have gone up on notice boards for many years that we can carry on doing it. Tell

students in advance that this is how their exam results will be published. If a student objects then you should not put their name on the list and advise them to see SDS for their results.

Examinations Scripts

Please note that the Information Commissioner's Office have produced a Data Protection Good Practice Note: Individuals' rights of access to examination records:
http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/data_protection_good_practice_note_access_to_exam_results.pdf

Universities do not have to provide exam scripts or the information recorded in them. However, Examiner's Comments are not covered by this exemption.

Examiners' Comments

Students have a right to see comments made by internal and external examiners. This means that comments must be intelligible and appropriate. It's helpful if examiners' comments are made on separate comment sheets, rather than directly on the scripts. Examiners need to be made aware of this in advance. If comments are handwritten and potentially illegible, it may be necessary to supply a typed version. If the examiners' comments have been made directly onto the exam script itself, the student cannot see the script so the comments would have to be transferred to a separate sheet that the student is allowed to see. ***Note:*** be careful not to write anything inappropriate on an Exam Script as this would have to be released to a student if requested by them, regardless of what is written!

Personal Data and Research

The Act applies to people collecting or using personal information as part of research. It's important that if you collect personal information as part of your research you explain to people what you are collecting, why you are doing it, what you will do with the information. Remember to tell them about all the things you'll do with their information. You may be collecting for a PhD thesis now, but if you are intending to publish that as a book later, then let people know.

There are some parts of the Data Protection Act that don't apply in quite the usual way when personal information is being collected for research. The main one is that personal information collected and used only for research purposes, can be kept indefinitely.

If you are doing social research you'll find more detailed ethical guidelines on the website for Research Governance Framework https://www.kent.ac.uk/res-local/policy/rgf/home.htm

Data Processing

A 'Data Processor' is someone other than a University of Kent staff member who processes data for and on behalf of the University. In such cases:

a) Ensure that the processing is carried out under a **contract:**

i) which is made under or evidenced in writing, and

ii) under which the data processor is to act only on instructions from the data controller, and

iii) which requires the data processor to comply with obligations equivalent to those imposed on a data controller by the **seventh principle**

b) Choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out**,** and

c) Take responsible measures to ensure compliance with those measures.

Employing Students

The University sometimes employees registered students. If you have a student employed in your section, school, or office, you need to make sure that as part of their induction they are told about the importance of Data Protection and understand that the information about students or staff that they have access to has to be treated confidentially.

Keeping Files on Individuals

The University keeps files of relevant information on staff and students. Everyone has a right to ask to see the information we keep about them. This means that you need to think carefully about the information you keep about people. It does not mean you can only ever write nice things about people on their file. It does mean that you should always use balanced and measured language in what you write. You should stick to facts, not opinions. Where you do need opinions then you should clearly state that's what they are. You should never make notes that are rude, offensive, derogatory or damaging.

Information about someone doesn't need to be in an actual physical file for them to ask to see it. It can be an e-mail or electronic document. This means that you should think carefully about what you put in e-mails. See our e-mail guidance (above) for more information.Personal Information on the University Website

The website is a public space. We generally publish information about people's official roles and functions. This helps those who need to deal with the University to find the right person to contact. It can also promote the University by letting people see which high profile academic staff we have within Schools.

It is important that anybody whose name and other information appears on the website knows that it is there and that there are ways for them to object and for the information to be removed if needs be. Personal information should not be published on the website. This applies to information that's on the open part of the website, and on the campus only sections. It applies to staff, students and anyone else whose details we put on the website.

Photographs

A photograph of a person is "personal data". Some Schools and sections in the University put photographs, and sometimes biographical information, about staff on notice boards and web pages. This is fine, but people have the right to refuse to have their photograph or personal information published in this way, even if the web page can only be seen by people on campus. It is best to ask people before you make their picture and details public.

Even though the information is likely to be work related and not to do with their private life it still counts as personal information.

Working from Home

If you work from home you still have to abide by the Data Protection Act. It is important that personal information isn't accidentally lost or revealed to anyone who doesn't have a right to see it.

The home VPN service allows you to access networked resources such as your files on the Kent network, e.g. files on Bodiam or in departmental folders. It is vital in this case that you do not save any personal data onto your home computer and you ensure that no-one else in your household is able to access any information. Also, before applying for use of the VPN Service you must have **up-to-date anti-virus software** installed and ensure you **apply all security updates** to your computer operating system. If you need to print something out when you are at home you should either shred it afterwards (if you are able) or bring it back to work for shredding.

If at all possible avoid taking personal data home. It is better to put it somewhere that can be accessed from home without having to be physically carried there in paper form or on a disk or memory stick. Consider finding a way to anonymise information that you need, to encrypt it or password protect it.

If people in your section or School regularly need to take personal information home with them then it's best to have a system to record who has taken information away, what information they took, when they took it, whey they took it, and when they bring it back again. This means you can be sure that you know where all of your information is.

For more information please visit www.ico.gov.uk or for any queries please contact the Data Protection Team datapro@kent.ac.uk

Appendices

Retention of Data

Personal data should be retained for at least a six year period unless such data is required to be retained for a longer period by regulation or statute. Heads of Sections/Departments/Schools, Deans and Directors shall be responsible for the monitoring of data and should determine what is to be held for more than six years or permanently.

Data	Held by	Retention period
Examinations composite marksheets / results	Centre Other	Permanent Permanent
Examination coursework / exam marksheets	Other	Permanent
References	Human Resources Other	6 years 6 years
Appeals / grievance hearings	Centre Other	6 years 6 years
Disciplinary action	Centre Other	6 years 6 years
Concession / medical evidence	Centre Other	6 years 6 years
Personnel Files	Centre Other	6 years 6 years
Tutorial / student files including UCAS forms		6 years
Finance Data	Centre Other	See attached Finance guidelines
Enquiry / applicant details		1 year
Interview notes		6 months
Student applications and criminal convictions	Centre	6 months

Documents marked with an asterisk (*) shall be retained within the Finance Division. However, the provisions of this Regulation apply equally to Academic Departments and Administrative Divisions, unless variations are agreed in writing by the Director of Finance. Any document not listed above should likewise be referred to the Director of Finance before any destruction or disposal is affected.

Discarding personal information too soon may be likely to disadvantage your business and, quite possibly, to inconvenience the people the information concerns. However, keeping personal data for too long may cause some problems:

- Increased risk that the information will go out of date, and that outdated information will be used in error – to the detriment of all concerned.
- As time passes it becomes more difficult to ensure that information is accurate.

- Even though you may no longer need the personal data, you must still make sure it is held securely.
- You must also be willing and able to respond to subject access requests for any personal data you hold. This may be more difficult if you are holding more data than you need.

We have already mentioned the links between the third, fourth and fifth data protection principles. So, for example, personal data held for longer than necessary will, by definition, be excessive and may also be irrelevant. In any event, it is inefficient to hold more information than necessary.

Retention of Finance Data

Financial and related documents shall be retained in a secure and accessible manner for the following periods of time which are in addition to the current financial year:

Type of Data	Retention period
Copy Official Orders (including cancelled orders)	3 years
Suppliers Delivery Notes	1 year
Employees Time Sheets*	1 year
Stores Requisitions/Issue Notes (including cancelled notes)	2 years
Suppliers Paid Invoices: Revenue Items Capital Items	 6 years 10 years
Inter-Departmental Transfers (including cancelled IDTs)	1 year
Records of Processed Invoice Batches	6 year
Till Rolls	6 year
Copy Official Receipts (including books)	6 year
Copy Pay-in Slips	6 year
General Correspondence (not central files)	2 year
Contract Documents*	All documents for a minimum of 20 years
Sundry Debtor Accounts*	10 years
Control Account Print Outs*	10 years
Control Account Reconciliations*	6 years
Paid Cheques*	6 years
Bank Statements*	6 years
Bank Reconciliation Statements*	6 years
Credit Transfer listings*	6 years

Cash Account Print Outs*	10 years
Cash Account Reconciliations*	6 years
Final Account Working Papers*	10 years
Payroll Input Forms*	6 years
Payroll Output	6 years
Income Tax Records*	6 years
VAT Records*	6 years

References

The Information Commissioner receives a lot of enquiries about:

- whether organisations can release a reference to the person who is the subject of the reference;
- how the Act applies to references; and
- the fact that references may have been given 'in confidence'.

The Data Protection Act is not very straightforward when it comes to references. The organisation supplying the reference does not have to show a copy to that person. However, the organisation receiving the reference does have to show a copy to the person, if they ask.

It is best to assume that at some stage any reference you write will be seen by the person you are writing about. There are two basic things to remember. The first is that you must distinguish carefully between your opinion and fact. So your opinion about a person might be that they are lazy and lack commitment. The fact will be that they only attended 30% of lectures in their final year or that they arrived late to work 12 days in the last month.

The second thing to remember is that you should only reveal what is necessary and what you know the data subject has already given out. So you would not reveal that a student had help during the course for dyslexia. If the student didn't ask for help with dyslexia until late in their studies, and you think that this affected the grade they got, then speak to the student and ask them if you can tell this to the prospective employer.

Sponsors

Financial sponsors can be individuals or organisations, or even a relative of the student. They often feel they must have a right to know certain information about the student. However this isn't necessarily the case.

We can sometimes provide limited, relevant information, although it will vary from case to case. The student and sponsor may have a contract that sets out what information can be shared, and we can give out information covered in such agreements. Otherwise it is best to ask the student's permission to give information to the sponsor or contact the Data Protection Officer.

Do you have to give a copy of a reference you have written?

If someone asks for a copy of a confidential reference you have written about them relating to training, employment or providing a service, you do not have to provide it because it is exempted in the Act. However, you may choose to provide the information. It would seem reasonable to provide a copy if a reference is wholly or largely factual in nature, or if the individual is aware of an appraisal of their work or ability.

Do you have to give a copy of a reference you have received from someone else?

References received from another person or organisation are not treated in the same way. If you hold the reference in a way that means it is covered by the Act, you must consider a request for a copy under the normal rules of access. An individual can have access to information which is about them, but may not necessarily have access to information about other people, including their opinion, provided in confidence.

The references you have received may be marked 'in confidence'. If so, you will need to consider whether the information is actually confidential. You cannot sensibly withhold information which is already known to the individual. Factual information such as employment dates and absence records will be known to an individual and should be provided. Information relating to performance may well have been discussed with the employee as part of an appraisal system.

Where it is not clear whether information, including the referee's opinions, is known to the individual, you should contact the referee and ask whether they object to this being provided and why.

Even if a referee says that they do not want you to release their comments, you will need to provide the reference if it is reasonable in all the circumstances to comply with the request without their consent. You should weigh the referee's interest in having their comments treated confidentially against the individual's interest in seeing what has been said about them.

When considering whether it is reasonable in all the circumstances to comply with a request, you should take account of factors such as:

- any express assurance of confidentiality given to the referee;
- any relevant reasons the referee gives for withholding consent;
- the potential or actual effect of the reference on the individual;
- the fact that a reference must be truthful and accurate and that without access to it the individual is not in a position to challenge its accuracy;
- that good employment practice suggests that an employee should have already been advised of any weaknesses; and any risk to the referee.

You should consider whether it is possible to keep the identity of the referee secret

Subject Access Request

This right, commonly referred to as subject access, is created by **Section 7** of the Data Protection Act. It is most often used by individuals who want to see a copy of information an organisation holds about them.

However, the right of access goes further than this and an individual who makes a written request and pays a fee is entitled to be:

- told whether any personal data is being processed
- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people
- given a copy of the information comprising the data
- given details of the source of the data (where this is available).

In most cases an organisation must respond to a subject access request promptly and in any event within **40 calendar days** of receiving it. However, some types of personal data are ***exempt*** from the right of subject access and so cannot be obtained by making a subject access request e.g. data used for the prevention or protection of crime.

Under the right of subject access, an individual is entitled ***only to their own personal data***, and not to information relating to other people (unless they are acting on behalf of that person e.g. solicitors). Neither are they entitled to information simply because they may be interested in it. So it is important to establish whether the information requested falls within the definition of ***personal data*** (see definitions).

The University of Kent charges a fee of £10 and any request made under the Data Protection Act will not be actioned on until the payment is received.

The second thing you are entitled to do before responding to a subject access request is to ask for information that you reasonably need to find the personal data covered by the request. Again, you need not comply with the subject access request until you have received this information.

The Act does not prevent an individual making a subject access request via a third party. Often, this will be a ***solicitor*** acting on behalf of a client, but it could simply be that an individual feels comfortable allowing someone else to act for them. In these cases, The Data Protection team will satisfy themselves that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a ***written authority*** to make the request or it might be a more general power of attorney.

Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The Act says you do not have to comply with the request if to do so would mean ***disclosing information about another individual*** who can be identified from that information, except where:

- the other individual has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without that individual's consent.

The Data Protection Act ***does not limit the number of subject access requests*** an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals. The Act says that you are not obliged to comply with an identical or similar request to one you have already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

You may transfer personal data to countries within the ***European Economic Area*** on the same basis as you may transfer it within the UK. However, you may only send it to a country or territory outside the EEA if that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal data. Read more about what this means in practice.

What do I do if I receive a request for personal data?

If you receive a request for personal information, you should always inform the data protection team datapro@kent.ac.uk as soon as possible. The Data Protection team are well equipped to deal with requests for personal detail.

If you are asked by the Data Protection team to provide data about a student then to team, then please ensure that you cooperate as quickly and as efficiently as possible. We have to ensure that we respond within the statutory time limit.