

Data Protection Policy

Author: David Palmer (ISD)

Date: 30 May 2012

Version: 1.0

This document defines the University's policy on data protection, and is based on the following principles.

- **The University will be compliant with all relevant legislation, particularly the Data Protection Act 1998, and will base its policies and practices on compliance with the eight Data Protection principles contained therein**
- **Ensuring compliance is a corporate responsibility of the University requiring the active involvement, of, and appreciation by, all staff at all levels of the organisation**
- **The University will strive to ensure best practice in regards data protection processes and procedures**
- **The University will strive to improve practices and procedures utilising external guidance, monitoring of jurisprudence in the areas, and adopting examples of best practice elsewhere**
- **The University will provide support and services to enable staff handling personal data to remain compliant with the legislation**

Version history

Version	Date	Note
0.1	30/05/12	First draft, adapted from Data Protection Briefing Paper
1.0	12/06/12	Approved by ISSC

Introduction

At UEA, personal data are held about students, staff and the public. UEA needs to hold information about its students and staff for reasons which include, but are by no means limited to, the following:

- the recruitment, employment and payment of staff
- the recruitment of students
- the administration of courses and examinations
- student welfare

Data may also be held on other individuals, such as visitors to UEA, suppliers, employees of other organisations who are involved in research contracts, and so on.

The Data Protection Act 1998 (DPA) places responsibilities and obligations on organisations which process data about living individuals. It also gives legal rights to individuals in respect of personal data held about them by others. The DPA may be found on the internet at www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm.

The University must have policies and procedures in place to ensure that we are compliant with our obligations under the Act that extend across the breadth of the staff and activities of the University.

Scope

This policy applies to:

- All students and staff employed by, or studying at UEA
- Any non-UEA staff with any degree of access and/or use of personal data held by the University
- All University activities that involve the processing of personal data as defined by the Data Protection Act 1998
-

Definitions

The following definitions apply to this policy:

- **the Act:** Data Protection Act 1998.
- **Data Security Breach:** A data security breach is the occurrence of any unauthorised or unlawful processing of personal data held by UEA, or the accidental loss, destruction of or damage to any such personal data.
- **Data Subject:** A *Data Subject* is a living individual who is the subject of personal data.
- **Data Controller:** A *Data Controller* is a person or organisation which controls the purposes and manner in which data are processed. UEA is a data controller, and the point of contact is the University's Information Policy and Compliance Manager.
- **Data Processor:** Any person or persons that process information on behalf of a data controller.
- **Data:** All information in **digital format, or manual data within a 'relevant filing system'**.
- **The Information Commissioner:** The *Information Commissioners Office (hereafter ICO)* is the supervisory authority, reporting directly to Parliament, which enforces and oversees the DPA and the FOIA. The Information Commissioner maintains a public register of data controllers. The process of adding an entry to the register is called *notification*. UEA's notification covers the classes of data which are processed, and is updated from time to time.
- **Information life cycle:** The time span that information processed by the University remains 'live' and relevant to the University and for which the University has obligations under this, or any other policy.
- **IPCM:** Information Policy and Compliance Manager.
- **Personal Data:** *Personal Data* are data which relate to a living and identifiable individual, including computerised data and some manual data (ie paper-based records, microfiche, etc). When the DPA was first passed into law, it covered data held in a "relevant filing system", which is defined in the DPA as a "set of information" which "is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible". However, the Freedom of Information Act 2000 (FOIA) modifies and extends the DPA to apply to "unstructured personal data". Unstructured personal data are any personal data which fall outside the definition of the relevant filing system given above.

The difference may be illustrated as follows. Personnel records are clearly part of a "structured filing system" as they are arranged by surname or employee number. However, a member of staff may serve on a university committee, and that person's name will appear in the minute book of that committee. The minute book is not structured by names, but by

the dates of committee meetings. Under the modification to the DPA, such data now fall within its remit, although a request for such unstructured data must contain a description of the data. In the example above, it would be reasonable for the person making the request to provide some dates or other information to enable the data to be tracked down.

- **Processing:** The term processing means, effectively, any action of any sort taken in regards personal data during the lifecycle of that personal data. This will include but is not limited to, obtaining, storing, adapting, transferring, transmitting, disposal and destruction.
- **Relevant filing system:** means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
- **Sensitive Personal Data:** The DPA recognises that certain types of personal data should be treated with particular regard. Such *Sensitive Personal Data* include data on racial or ethnic origin; political opinions; religious beliefs; membership of a trade union; physical or mental health or condition; sexual life; and criminal offences.
- **Subject Access request (SAR):** The means by which any individual exercises the right, pursuant to section 7 of the Data Protection Act of any individual to see a copy of the information an organisation holds about them. A SAR can include the following elements:
 - a request to be told whether any personal data is being processed;
 - a request to be 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;
 - a request to be given a copy of the information comprising the data; and
 - a request to be given details of the source of the data (where this is available).
- **UEA:** The University of East Anglia.

Aims

The aims of the Data Protection Policy are to:

- Set out the obligations of the University in regards data protection
- Establish the guiding principles for the University's actions in this area
- Provide a Policy framework to ensure local compliance with the Act

Policy statements

Notification

- The University will comply with the notification obligations placed upon it by the Act and associated regulations; specifically renewing notification with the ICO yearly, and ensuring that the notification is current and accurate. To further the latter, the University will conduct a comprehensive review of its notification no later than every 5 years, and more frequently should the activities or data holdings of the University so demand.

Personal data held by UEA

- Data are collected from students at various stages. Examples include, but are not restricted to:
 - data on applications (often transferred to UEA from UCAS)
 - blue registration data
 - applications for financial aid
 - data held by the Dean of Students' Office in connection with student welfare
- Data are also added subsequently to students' records, for example:
 - marks statements
 - changes of address
 - final degree results
 - medical certificates
 - concession or intercalation requests
- The Human Resources Division collects data on staff and creates a Personnel File for every member of staff. Some of this information will also be held by individual administrative units within the University. Such data will include:
 - applications for posts at UEA. For unsuccessful candidates, these data are generally destroyed once the appointment process is complete.
 - terms of appointment.
 - annual review
 - promotions
- All staff and students are responsible for ensuring that any information that they provide to UEA in connection with their employment or study is accurate and up-to-date, and for informing UEA of any changes to that information, such as changes of address.
- Upon graduation, some information is passed to the Alumni Association to allow them to contact graduates about UEA events, products, services and for survey purposes. Central systems also retain basic graduate student data regarding academic progress to verify awards and to provide a record of lifelong learning.

Processing obligations – general

- *Data Protection principles in general*
 - Under the DPA, personal data must be processed in accordance with the following eight Data Protection Principles. These principles are contained within Schedule 1 of the Act and are the fundamental obligations imposed by the Act in regards the processing of personal data. The term *processing* has a very wide application which includes the mere fact of holding data about a living individual, as well as the alteration, disclosure and destruction of personal information. The eight Data Protection Principles state that data must:
 1. be obtained and processed fairly and lawfully and only if certain conditions are met
 2. be obtained for specified and lawful purposes
 3. be adequate, relevant and not excessive for those purposes
 4. be accurate and up-to-date
 5. not be kept for longer than is necessary
 6. be processed in accordance with the rights of data subjects
 7. be kept safe from unauthorised access, loss or destruction
 8. not be transferred to countries outside the European Economic Area, unless to countries with equivalent levels of data protection.

- *The First Principle - Fair processing*

- The requirement for 'fair processing' is set out in the first data protection principle and is the most important principle in regards the processing of personal data. In essence, this principle demands, and it is UEA policy that, all personal data for which the UEA is data controller will be processed in line with the expectations of the relevant data subjects, and that all data subjects will have adequate notice of any processing undertaken by UEA.
- In practice, many of the problems associated with compliance with the Act can be avoided if consent to store and handle the information is obtained from the individual at the time of data collection and, thereafter, the organisation which collected the information adheres to the terms of consent.
- When a student registers at the beginning of his or her course, he or she is issued with a [data protection notice](#). The notice sets out the types of data which are being collected and the uses to which these will be put, including transfers to other organisations such as the Higher Education Statistics Agency. It also informs the student that, by signing the registration form, he or she consents to the processing of those data, for purposes connected with the legitimate activities of UEA.
- For staff, a data protection notice is included on application forms for employment at UEA which sets out the data which are collected, the uses to which they will be put, and seeks consent for their processing. There is also a [notice for successful applicants](#), when they join UEA.
- Particular attention is drawn to the collection of data on Ethnic Origin and Disability, since these are among the types of *sensitive data* defined in the DPA. Explicit consent must be obtained for the processing of sensitive data, and this is made clear in the notices issued to staff and students, which explain that, by providing these data, the staff member or student consents to the processing of his or her data within carefully-defined limits. We cannot force an individual to provide these data, and he or she is quite at liberty to refuse to provide them on the application or registration form (which means, effectively, that consent for their processing has been withheld).

- *The Seventh Principle - Data Security*

- Adequate data security is essential to meet the requirements of the 7th Data Protection principle. Where anyone subject to this Policy is in possession of personal data they must:
 - Ensure that the personal data is technically stored and handled in line with approved UEA [data security standards](#) and processes.
 - Ensure that organisation measures are in place to guard against unauthorised or unlawful damage or destruction of the personal data. Such measures could include: restricting access to the data to minimum number of persons possible, ensuring that all digital personal data is password protected wherever it may reside, ensuring that any personal data are not left 'in the open' either in paper form, or on a screen in digital form, ensuring that access to the area in which the personal data is stored is restricted to only those persons who need to be there, minimise the need for transfer of the data, if transfer is required, ensure that UEA data security protocols are in place and observed.
 - Take steps to provide an adequate level of security and DPA training is provided to anyone with access to the personal data, inclusive of anyone outside of UEA that may have access to the data.

- The IPCM will work with appropriate units within ISD to ensure that all technical security requirements are met and will work with the appropriate internal authority to ensure that appropriate organisational measures are in place.
- *Other processing obligations*
 - Staff should ensure that personal data are:
 - processed only for the purposes for which they were collected (note that simply holding data on file counts as processing)
 - not divulged to third parties without the subject's consent
 - relevant and up to date
 - disposed of as confidential material when they are no longer needed for the purposes for which they were collected and in line with [UEA records management guidelines](#) and practices
 - not transferred outside the EEA unless there are adequate measures in place that ensure a level of protection equivalent to that afforded by the Act
 - To take an example, a student's file should only contain those data which are necessary at a particular time. If a student is currently interrupting his or her studies because of illness, it may be necessary to keep copies of medical certificates, contact details and so on. But in ten years' time, when that student requests a replacement degree parchment, the fine detail will no longer be required - just a note of the fact that "the student was away from UEA for a year for medical reasons". Some data (such as the student's final degree result) must be kept permanently. Further advice is available from the Student Records Office in the Registry.

Data Sharing

- Information should not be transferred to any 3rd party unless such a transfer is authorised by the Act itself, by other statute, or by the UEA Student Data Protection Notice or UEA Staff Data Protection Notice.
- The Act authorises release to 3rd parties without proper notice to the data subject under certain limited circumstances such as
 - Detection or prevention of crime, apprehension of offenders
 - Schedule 2 conditions
 - Protection of the vital interests of the data subject
 - Pursuant to a contract to which the data subject is a party
 - Pursuant to a legal obligation imposed upon the UEA
 - Where necessary for the pursuit of the legitimate interests of the UEA or any 3rd party save where such processing is unwarranted by prejudice to the rights, freedoms or legitimate interests of the data subject
- Any proposed data sharing must be reviewed by the IPCM who has the responsibility of determining whether, on the facts of the case, a data processing agreement is warranted. As a general rule, one off, ad hoc data sharing events will not require an agreement whilst any ongoing data sharing will require such an agreement.

- If a data processing agreement is warranted, the IPCM will work with the relevant line manager with operational responsibility for the data sharing to draft and agree an agreement that assures that the University meets its compliance obligations.

Specific UEA-related processing policies

- ***References***

- It is relatively common for staff or students to request access to personal references written at the time of their application for employment or study at UEA, or for employment or study elsewhere. This is an area where a specific exemption is written into the DPA: references *given by* UEA (the *Data Controller*) are exempt from the subject access provisions.

Thus, students and staff of UEA cannot apply to see references provided by UEA staff and sent to another organisation. They may, however, apply to the organisation to which the reference has been sent.

- Similarly, they may apply to UEA to see references which have been *received by* UEA and which may be held in (say) a Personnel File. These references *received by* UEA are treated as any other items in a file, and we would follow the normal procedure regarding handling subject access requests by data subjects. It is worth bearing in mind that anonymisation is unlikely to be effective where references are concerned, and it is very likely that we would seek the consent of the author before releasing them, before deciding whether or not it was reasonable to release the reference "in all the circumstances".
- The Information Commissioner has advised that, where a reference has had an adverse effect on the subject of the reference, the subject's right of access will normally outweigh any other circumstances, even if the reference was given in confidence, and the author has expressly refused his or her consent to its disclosure.

- ***Research***

- The Act allows certain exemptions in the case of personal data which are collected and processed for research purposes, or for historical or statistical purposes. If the processing is *only* for the purposes of research (and is not used to support decisions about individuals) then
 - the data can be kept indefinitely.
 - subject access does not have to be granted, as long as the results of the research are anonymised.
- This is of course very common in the case of medical research papers which often refer to Ms A, Mr B, *et al.*
- Care should be taken if a key is retained which enables anonymised data to be decoded and therefore attributed to individuals. An appropriate level of care would exist if the key was only known to those individuals directly involved in the research, and kept under lock and key, and separate from the usual location of the anonymised data. Care should also be taken when students are conducting research involving personal data as part of their studies. In such cases, UEA remains the data controller and is responsible for the student's adherence to the DPA.
- Many research projects in the health area must first be approved by an Ethics Committee, and one of the conditions of such approval is that the advice of the

IPCM has been sought. The IPCM frequently offers such advice and often asks to see a copy of the research protocol.

- *Examinations*
 - The DPA contains a specific exemption for "personal data consisting of marks or other information processed by a data controller for the purpose of determining the results of an academic, professional or other examination or of enabling the results of any such examination to be determined". When a subject access request is made before the day on which the results of the examination are announced, such data may be withheld until five months from the date of the request, or the end of forty days beginning with the date of the announcement of the examination results, whichever is the earlier. The purpose of this provision is to prevent the release of examination marks until the assessment process is complete
 - Information recorded on an examination script by an examination candidate is specifically exempt from the provisions of the DPA. However, comments written on the scripts by examiners are not exempt. Students may apply to see these comments in the same way that they may apply to see other data, although such comments may not be released until the results of the examination are known. Examiners should endeavour to provide comments in such a way as to make them easily severable from the script itself, preferably by use of a separate cover sheet.
 - According to UEA's custom and practice, Pass Lists showing the results of undergraduate-level final assessments will be posted on notice boards, and will also be on display at Registry reception. The University will inform students by way of the Student Data Protection Notice that the results of the final assessment will be published.

System and Process Assessment

- Any system, project, process, or information holding within the University that involves personal data must be compliant with our obligations under the Act and an assessment and evaluation of compliance will be necessary.
- Privacy Impact Assessment – in the case of major systems, a full, or truncated Privacy Impact Assessment may be required. This will only be required in the case of major initiatives involving substantial amount of personal data or particularly sensitive or potentially risky processing of data. The ICO provides brief guidance on this process (see: http://www.ico.gov.uk/for_organisations/guidance_index/~media/documents/library/Data_Protection/Practical_application/PRIVACY_IMPACT_ASSESSMENT_OVERVIEW.ashx)
- A UEA-generated checklist of data protection compliance should be completed at the commencement of any project or system to identify data protection issues, risks and processes that need to be addressed. The checklist is available from the Strategy, Policy and Compliance unit within ISD.
- For other smaller processing issues, advice and guidance will be available from the IPCM with assistance from other members of the Strategy, Policy and Compliance unit. Where such advice and guidance is given, every opportunity will be explored to expand the knowledge and awareness of the individual or organisational unit seeking the advice and guidance.

Training and Awareness

- Training and awareness is essential for the University to be in a position to meet its obligations under the Act.

- ISD has primary responsibility for ensuring that adequate and appropriate training and awareness exist within the University, with the IPCM taking the lead role within ISD.
- All employees, upon obtaining employment with the University, will receive general information on the Act and our obligations thereunder as a component of the induction documentation and process.
- The IPCM is responsible for creating and maintaining both web-based and print material for reference and awareness. This post is also responsible for presenting scheduled training to staff via the CSED training program, scheduled training to the student population, particularly PGR students, and providing ad hoc training where appropriate.
- The IPCM, in conjunction with relevant University units, will identify those roles requiring particular training and awareness of data protection responsibilities and will work with relevant unit to ensure that adequate and appropriate training is provided. Monitoring of the effectiveness of training and awareness activities should be undertaken and maintained consistently.

Data Breach Management

- It is the responsibility of all UEA staff to avoid data security breaches but where one does occur, the affected unit, Faculty or individual must and will report the breach to the IPCM.
- Any personal data breaches will be handled in accordance with current guidance from the Information Commissioner's Office and investigation of any breach will initially be the responsibility of the IPCM.
- Any breach will be immediately reported to the Assistant Director, Strategy, Policy and Compliance within ISD and any decision regarding the notification of either the ICO or affected parties of any breach will be taken on his authority.
- The general procedure in the case of a data security breach will follow ICO guidelines and focus on the proper completion of four stages of breach management:
 - Containment and recovery
 - Assessment of ongoing risk
 - Notification of breach
 - Evaluation and response
- It is the responsibility of the IPCM to ensure that all four stages are addressed. The Assistant Director Strategy, Policy and Compliance has the responsibility of signing off that each stage has been successfully undertaken and completed.

Data Subject access requests (SAR)

- Persons about whom UEA holds data (*Data Subjects*) may make a request (a *Subject Access Request*) to see those data, and to receive or view copies of those data in permanent intelligible form (print-outs or photocopies). Students, staff or any individuals external to UEA who wish to make a Subject Access Request should be directed to the appropriate [request page](#) within the Data Protection web pages for the University.
- The IPCM, with the assistance of other members of the Strategy, Policy and Compliance unit, has the responsibility to co-ordinate the request centrally. Requests must be made in writing on the standard application form and accompanied by the standard fee of £10. Persons making a subject access request will also be required to confirm their identity. The DPA provides that UEA must respond to a formal request within 40 calendar days.

- The detail of the processes and procedures to be followed in administering a Subject Access request are set out in the Data Protection SAR Operations Manual, available from ISD.

Ownership

The Strategy, Policy and Compliance unit within ISD have ownership of this Policy.

Responsibilities

Within this policy, the following individuals have the following responsibilities:

Responsibility	Owner
Administration of subject access requests, training and awareness of staff, response to data protection inquiries from staff & students, investigation and management of data security breaches	Information Policy and Compliance Manager (IPCM)
To assist the IPCM with subject access request administration	ISD Project Manager
Overall responsibility for Data Protection Policy, authorisation of actions related to a data security breach, management and oversight of IPCM	Assistant Director Strategy, Policy and Compliance
Strategic liaison regarding data protection with other UEA units, ISD approval of data protection policies	Director of Information Services
Institutional approval of Data Protection policies	Information Services and Strategy Committee
Personal data to be handled in line with University policy, best practice, and the Act	Staff and students handling personal data

References

This data protection policy is supported within the context of the following pieces of legislation, professional standards, and University documents:

- Data Protection Act 1998
- Data Protection and Freedom of Information Fees Regulations 2004
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- UEA Freedom of Information Policy

Review

Annual; by IPCM in consultation with the Assistant Director Strategy, Policy and Compliance and with the Director of Information Services.