DATA PROTECTION AND DATA SECURITY POLICY

Purpose

1. This document defines the University of Suffolk's policy on data protection and data security and is based on the following principles:

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

Introduction

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

- the recruitment of students;
- the recruitment, employment and payment of staff;
- the administration of courses and assessment of student work;
- student welfare.

Data may also be held on other individuals, such as enquirers to courses, visitors to the University, suppliers, employees of other organisations who are involved in the delivery of University of Suffolk courses, research contracts, and so on.

3. 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.

4. The University of Suffolk is required to have policies and procedures in place to ensure compliance with its obligations under the Act that extend across its students, staff and the activities of the Institution.

Scope

5. This policy applies to:

- All students studying at the University of Suffolk, including applicants to its courses.
- All staff employed by the Institution.
- Any non-University staff with any degree of access and/or use of personal data held by the Institution.
- All institutional activities that involve the processing of personal data as defined by the Data Protection Act 1998.

Definitions

6. The following definitions apply to this policy:

- **The Act**: Data Protection Act (DPA) 1998.
- **Data security breach:** Any occurrence of any unauthorised or unlawful processing of personal data held by the University of Suffolk, or the accidental loss, destruction of or damage to any such personal data**.**
- **Data subject:** A living individual who is the subject of personal data.
- **Data controller:** A person or organisation which controls the purposes and manner in which data are processed. The University of Suffolk is a data controller, and the point of contact is the Academic Registrar.
- **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 (ICO):** The supervisory authority, reporting directly to Parliament, that enforces and oversees the DPA, and other information related legislation. The ICO maintains a public register of data controllers. The process of adding an entry to the register

is called *notification*. The University'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 of Suffolk remains 'live' and relevant to the Institution (inclusive of its disposal or destruction) and for which the Institution has obligations under this, or any other policy.
- **Personal data:** Data which relate to a living and identifiable individual, including computerised data and some manual data (i.e. 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 minutes of that committee. The minutes are not structured by names, but by the dates of committee meetings. Under the modification to the DPA, such data now fall within its remit**.**
- **Processing:** An 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:** 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 data include 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 DPA 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).

Aims

7. The aims of the Data Protection and Data Security Policy are to:

- Set out the obligations of the Institution with regard to data protection and data security.
- Establish the guiding principles for the Institution's actions in this area.
- Provide a policy framework to ensure local compliance with the DPA and the Institution's requirements in respect of data security.

Policy statements

Notification

8. The University of Suffolk 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 Institution so demand.

Personal data held by the University of Suffolk

9. Data are collected from students at various stages. Examples include, but are not restricted to:

- data on applications (often transferred to the University of Suffolk from UCAS)
- enrolment and registration data
- applications for financial aid
- data held by Student Services in connection with student welfare

10. Data are also added subsequently to students' records, for example:

- marks and progression statements;
- changes of address;
- final degree results;

- medical certificates;
- extenuating circumstances applications;
- payment of fee and debt status.

11. The Directorate of Human Resources collects data on staff and creates a personnel file for every member of University of Suffolk staff. Some of this information will also be held by individual administrative units within the Institution. Such data will include:

- applications for posts at the University of Suffolk;
- terms of appointment;
- appraisal;
- promotions;
- leave records.

12. All staff and students should ensure that any information that they provide to the University in connection with their employment or study is accurate and up-to-date. The University of Suffolk has ultimate responsibility for ensuring the personal information it holds is accurate and up to date.

13. Upon graduation, some information is passed to the University of Suffolk Alumni Association to allow that body to contact graduates about University of Suffolk 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

14. 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 with regard to the processing of personal data. The term *processing* has a 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; and
8. not be transferred to countries outside the European Economic Area (EEA), unless to countries with equivalent levels of data protection.

The first principle - fair processing

15. The requirement for 'fair processing' is set out in the first data protection principle and is the most important principle with regard to the processing of personal data. In essence, this principle demands, and it is the Institution's policy that, all personal data for which the University is the 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 the Institution.

- If any academic or professional services area is planning to collect personal data from anyone, consent to store and handle the information must be obtained from the individual at the time of the data collection. Advice on writing the appropriate privacy notices is available from the Head of Management Information.
- 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 (HESA). 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 the Institution.
- For staff, a data protection notice is included on application forms for employment at the University of Suffolk 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 the Institution.
- Particular attention is drawn to the collection of data on ethnic origin, disability and other protected characteristics, 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. An individual cannot be forced to provide these data, and he or she is 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

16. Adequate data security is essential to meet the requirements of the seventh 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 University of Suffolk data security policies and processes;
- ensure that Institutional 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;, minimising the need for transfer of the data, if transfer is required; and ensuring that University of Suffolk data security protocols are in place and observed;
- take steps to provide an adequate level of training in DPA and information security to anyone with access to the personal data, inclusive of anyone outside of the Institution that may have access to the data.
- The Academic Registrar will liaise with the Director of IT Services to ensure that all technical security requirements are met and that appropriate organisational measures are in place.
- Appendix 1 provides additional guidance on the secure use of mobile devices.

Other processing obligations

17. 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, accurate and up to date;
- adequate but not excessive for the stated purpose;
- disposed of as confidential material when they are no longer needed for the purposes for

which they were collected and in line with University of Suffolk data retention procedures;

- 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.

Data sharing

18. Information should not be transferred to third party unless such a transfer is authorised by the Act itself, by other statute, or by the University of Suffolk Student Data Protection Notice or the University of Suffolk Staff Data Protection Notice.

19. The Act authorises release to third parties without notice to the data subject under certain limited circumstances such as:

- detection or prevention of crime, apprehension of offenders;
- 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 Institution;
- where necessary for the pursuit of the legitimate interests of the Institution or any third party save where such processing is unwarranted by prejudice to the rights, freedoms or legitimate interests of the data subject.

20. Any proposed data sharing that does not meet the above conditions must be reviewed by the Academic Registrar 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 on-going data sharing will require such an agreement.

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

22. Data that is appropriate under the Act to share must be transmitted in the most secure form available. As far as possible data should be transmitted solely over the secure University of Suffolk network and the transmission of data via paper, post or independent electronic devices is strongly discouraged. The University of Suffolk IT network is such a secure system, with fully managed access control, backup and recovery processes in place.

23. The University of Suffolk Learning Network and the Students' Union are separate institutions that provide separate notifications to the Information Commissioner and are therefore responsible for their own compliance with the Act. However, these organisations reserve the right to share information with the University of Suffolk and each other as necessary to pursue their legitimate interests, or to ensure the smooth operation of procedures and practices in the interests of students, staff and other individuals connected to the Institution. Any disclosure of personal data is made in accordance with the Act and the Student Data Protection and Staff Data Protection notices and in the Framework Collaboration Agreement between the University of Suffolk and the Learning Network.

24. Where it is legitimate to share personal data with external organisations, the following hierarchy of actions should be adhered to:

- Data should be uploaded via a secure portal wherever possible; most organisations using this method publish details of security systems on their websites.
- Where there is no secure portal, data should be transmitted electronically (for example, as files, databases, PDF files, images) over secure networks. These files should be encrypted and, if so, then email is acceptable for such transmission. Where the transmission of large sets of data is unavoidable, IT Services can advise how this is best achieved.
- Data should be accessed through the host information system directly (if working away from the office, this may be done via a remote connection).
- If it is unavoidable to share paper copies of sensitive data, they should be mailed in securely sealed envelopes and sent by courier or registered post. An individual's personal data in the form of, for example, assessment results or letters of appointments, may be sent in sealed envelopes using normal postal systems.
- Particular care should be taken when transmitting sensitive data to unfamiliar recipients. Wherever possible the authenticity of the recipient should be checked with a known contact at the recipient organisation.

Specific University of Suffolk -related processing policies

References

25. 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 the University, or for employment or study elsewhere. This is an area where a specific exemption is written into the DPA: references *given by* the University of Suffolk (the *data controller*) are exempt from the subject access provisions. Thus,

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

26. Similarly, they may apply to see references which have been *received by* the University and which may be held in (say) a personnel file. These references *received by* the University 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 the Institution 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".

27. The ICO 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

28. 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.

29. This is common in the case of medical research papers which often refer to Ms A, Mr B, *et al*.

30. 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 securely, 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, the University of Suffolk may be the Data Controller and responsible for the student’s adherence to the DPA.

31. Many research projects involving human subjects must first be approved by an Ethics Committee, and one of the conditions of such approval is that the advice of the Academic Registrar has been sought. As part of this role, the Academic Registrar may ask to see a copy of the research protocol.

Examinations and assessment outcomes

32. 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 or assessment 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 or assessment results, whichever is the earlier. The purpose of this provision is to prevent the release of examination or assessment marks until the assessment process is complete.

33. 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 separated from the script itself, preferably by use of a separate cover sheet.

System and process assessment

34. Any system, project, process, or information holding within the Institution that involves personal data must be compliant with the Institution's obligations under the Act and an assessment and evaluation of compliance will be necessary.

35. 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.

36. A University of Suffolk-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 Head of Management Information.

37. For other smaller processing issues, advice and guidance will be available from the Head of Management Information. 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

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

39. The Academic Registrar has primary responsibility for ensuring that adequate and appropriate training and awareness exist within the Institution, working closely with the Director of Human Resources and the Director of IT Services.

40. All employees, upon obtaining employment with the University of Suffolk, will receive general information on the Act and the Institution's obligations thereunder as a component of the induction documentation and process.

41. The Academic Registrar has overarching responsibility for the creation and maintenance of web-based and print material for reference and awareness. This post is also responsible for ensuring that scheduled training is available to staff and students and providing ad hoc training where appropriate.

42. The Academic Registrar, in conjunction with relevant University departments, will identify those roles requiring particular training and awareness of data protection responsibilities and will work with the relevant department 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

43. It is the responsibility of all University of Suffolk staff to avoid data security breaches, but where one does occur, the affected department, Faculty or individual must report the breach to the

Head of Management Information at the earliest possible opportunity.

44. Any personal data breaches will be handled in accordance with current guidance from the ICO and the disciplinary procedure, and investigation of any breach will initially be the responsibility of the Head of Management Information or nominee.

45. Any decision regarding the notification of either the ICO or affected parties of any breach will be taken on the authority of the Academic Registrar.

46. 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 on-going risk
- Notification of breach
- Evaluation and response

47. It is the responsibility of the Head of Management Information to ensure that all four stages are addressed. The Academic Registrar is responsible for authorising any actions and signing off that each stage has been successfully undertaken and completed.

Data Subject Access Requests (SAR)

48. Persons about whom the University of Suffolk holds data (*data subjects*) may make a Subject Access Request (SAR) 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 the Institution who wish to make a SAR should be directed to the appropriate page of the University's website.

49. The Head of Management Information, in liaison with the Academic Registrar's Professional Assistant, has the responsibility to co-ordinate the request centrally. Requests must be made in writing preferably on the standard application form and accompanied by the standard fee of £10. Persons making a SAR will also be required to confirm their identity. The DPA provides that the University must respond to a formal request within 40 calendar days.

50. The detail of the processes and procedures to be followed in administering a SAR are set out

in the Data Protection SAR Procedure available from the Head of Management Information.

Data storage, retention and disposal

51. Adequate data security is essential to meet the seventh principle of the Act and the following safeguards are in place at an organisational level:

- Each of the corporate systems at the University of Suffolk has an underlying database with built-in security, backed up by copying to secure storage each night.
- Firewalls limit external access to the University of Suffolk network. Only authorised users with University logins have access to the network: enrolled students, staff and trusted visitors.
- Server rooms are strictly controlled access areas.
- The login gives access to the University of Suffolk network. Staff passwords expire after a defined period and have to be changed by the user. Student passwords do not expire; however students are advised to change them regularly. Both staff and students are advised to change their passwords immediately if they believe their details have been compromised.
- Although workstations automatically lock if left inactive for a specific period, users are advised to always lock their workstations when moving away from their desk (windows key and L on a PC).
- Data stored on a network drive is backed up each night.

52. A range of specialist databases exist which contain varying levels of personal and sensitive information. The following should be adopted as good practice:

- Each database should be held in a separate directory on the main University of Suffolk network drive and be password restricted to an authorised individual or group.
- The database itself should be password protected by the system administrator.
- All other personal or sensitive data that may be held in local, small-scale documents, for example spreadsheets and word documents, must be password protected and restricted to essential users.
- Personal or sensitive data should never be copied to a lap-top computer for local processing without the express permission of the system owner and only in exceptional circumstances. Whilst University laptops are password protected, they can be vulnerable to a determined hacker. Equally, personal or sensitive data should not be stored on flash-drives, CD-ROM or other external devices.

53. Data at the University of Suffolk are retained and disposed of according to need. The overarching principle is that data should only be retained and stored for as long as such data have a legitimate purpose, and thereafter they should be disposed of securely. Each Faculty and professional service area of the Institution holds a Data Retention Schedule which specifies the nature of the data retained, the retention period, the reason for retention, and the action to be taken at the end of the retention period, including how the data are to be disposed of.

54. At the end of the retention period, data should be disposed of and/or destroyed. Manual files should be shredded and disposed of in designated confidential waste sacks if appropriate. Electronic data should be deleted from central systems by the individual responsible for the data after liaising with the IT Services team.

Complaints

55. Individuals concerned about any aspect of the management of personal data at the University may raise their concerns in the first instance with the owner of the corporate system involved (see Appendix 2) or the Head of Management Information. If the concern cannot be resolved, then a formal complaint may be made in accordance with the Complaints Procedure, using the form available on the University of Suffolk website. If an individual, having followed these procedures, is not satisfied that their complaint has been properly dealt with they may contact:

The Information Commissioner (ICO)
Wycliffe House
Water Lane
Wilslow, Cheshire, SK9 5AF

Responsibilities

56. Within this policy, the following post-holders have these responsibilities:

Responsibility	Owner
Administration of subject access requests, response to data protection enquiries from students.	Head of Management Information in liaison with the Academic Registrar's Professional Assistant
Initial investigation and management of data security breaches.	Head of Management Information

Overall responsibility for Data Protection and Data Security Policy, authorisation of actions related to data security breaches, management and oversight of the Head of Management Information, raising awareness of DPA across the Institution, and the provision of training and information for staff and students	Academic Registrar
Overall responsibility for those aspects of data security relating to University of Suffolk information technology systems	Director of IT Services
Strategic liaison regarding data protection and data security with the Executive and the University of Suffolk Board	Registrar and Secretary
Institutional approval of Data Protection and Data Security Policy	Executive Board and Senate
Personal data to be handled in line with the University of Suffolk Data Protection and Data Security Policy, best practice and the Act	Staff and students handling personal data

Review

57. The policy will be reviewed in accordance with the corporate policy review schedule or when legislation is amended (whichever is the sooner) by the Academic Registrar in consultation with the Director of IT Services and Head of Management Information.

References

58. The policy is supported within the context of the following pieces of legislation and University of Suffolk policies:

- Data Protection Act 1998
- Data Protection and Freedom of Information Fees Regulations 2004
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Privacy and Electronic Communications Regulations 2003
- University of Suffolk Code of Practice for Managing Freedom of Information Requests

- University of Suffolk ICT Acceptable Use Policy
- University of Suffolk Data Retention Schedules (departmental)

Appendices

59. The policy is supported by the following documents:

- Appendix 1: Secure use of mobile devices;
- Appendix 2: List of corporate system owners and administrators;
- Appendix 3: Staff data protection notice;
- Appendix 4: Data Subject Access Request (SAR) Form (Staff);
- Appendix 5: Student data protection notice;
- Appendix 6: Data Subject Access Request (SAR) Form (Student);
- Appendix 7: Staff data collection consent – extract from University of Suffolk Contract of Employment (staff);
- Appendix 8: Student data collection consent – extract from Student Enrolment Form;
- Appendix 9: Data protection guidance for staff.

Appendix 1: Secure use of mobile devices

1. Purpose

The secure use of mobile devices addresses, in particular, the Seventh Principle – Data Security and the Data Protection Act sets out the principles, expectations and requirements relating to the use of mobile devices and other computing devices which are not permanently located on University of Suffolk premises.

This document should be read in conjunction with the Data Protection and Data Security Policy.

2. Definition

A mobile device is defined as a portable computing or telecommunications device which can be used to provide some of the functions typically associated with a desktop PC, such as storing or processing information. Examples include laptops, netbooks, tablets, smartphones, removable storage media (USB sticks/external hard drives) and wearable devices (Apple Watch/Pebble). As technology moves forwards this list is likely to expand.

3. Scope

All staff at the Institution including contractors, service providers and other organisations that use mobile devices to access University of Suffolk networks or information must comply with Institutional policy. It covers all mobile computing devices whether personally owned, supplied by the University or provided by a third party. Non mobile devices that are not located on University premises and are used for accessing University of Suffolk networks or information are also in scope.

It does not cover personal devices of students at the University of Suffolk, only any device loaned to the student by the University, although it is suggested that students follow the policy to ensure the security of the data and information on their device.

4. Personally owned devices

Whilst the University does not require its staff to use their own personal mobile devices for work purposes, it is recognised that there is demand for this and it is often beneficial. The use of these devices is permitted subject to the following requirements and guidelines. Users must at all times give due consideration to the risks of using personal devices to access University of Suffolk data and information:

Requirements

- An appropriate password/passcode must be set for all accounts on that device.
- A password protected screen saver or screen lock must be used.
- All devices must be set to lock automatically after a set period (5 minutes maximum) and require a password to unlock after this time.
- The device must run the latest version of the operating system and be updated with software updates/security patches in a timely fashion.
- All mobile devices used to access or store sensitive/confidential information must have the ability to be located and be remotely wiped, particularly smartphones and tablets.
- In the case of storage media all sensitive/confidential data stored on the device must be encrypted.
- Any devices at risk of malware infection must run anti-virus software.
- Any device used for this purpose should only be used by an authorised person. If family or friends are to use the device then it must be managed in such a way that others do not have access to this information.

Guidelines

- Do not undermine the security of the device for example by Jail Breaking an iPhone.
- Minimise the amount of sensitive/confidential data stored on the device.
- If a device needs to be repaired, ensure that the company you are has an agreement in place which guarantees the security of any data on the device.
- Do not leave devices unattended where there is a risk of theft.
- Be aware of people around you when entering passwords or using the device.

5. University of Suffolk owned devices

The University of Suffolk will occasionally supply mobile devices to staff as required for their work. Where possible these devices will be configured in the same way as those which are permanently located on University premises. Occasionally it is not possible to configure the device for the user, and it will be the responsibility of the user to set the configuration.

Whether the device is configured by the University of Suffolk prior to release or not, the requirements and guidelines listed above should be followed and the following additional requirements apply to any University owned device:

- Non-members of the Institution must not make any use of the supplied device.

- No unauthorised changes must be made to the supplied device.
- All devices must be returned to the University of Suffolk when they are no longer required or are in need of repair.

6. Third party devices

No staff should use any mobile device or other device that is for public use to access University of Suffolk networks or information. This includes public libraries or cyber cafes.

7. Lost equipment

Should a staff member at any time lose equipment that they believe contains sensitive/confidential content or allows access to the University of Suffolk network, this must be reported immediately to IT Services who can advise on the best course of action.

Appendix 2: List of corporate system owners and administrators

April 2016

System	System owner
Active Directory/Account Provisioning Service	Director of IT Services Administrator: (Head of IT)
CAFM	Director of Estates
Enterprise Service Desk	Head of Academic Services and Infozone
External Examiners	Head of Registry
Facilities Management	Director of Estates
Heritage (Library Systems)	Head of Learning Services
Intranet/Applicant Portal	Director of External Relations
Learn/Blackboard VLE	E-learning Development Manager
QLx (Finance)	Director of Finance and Planning
ResourceLink	Director of HR Administrator: Head of HR Operations
SITS	Head of Management Information Administrator: Student Systems & Reporting Manager
TRAC System	Director of Finance and Planning
University of Suffolk website	Director of External Relations

Appendix 3: Staff data protection notice

The University of Suffolk has a notification under the Data Protection Act 1998 to hold personal data about all members of its staff for the purposes of recruitment, appointment, training, remuneration, promotion and other employment related matters, including health and safety. The information is held in a variety of formats, including centrally managed databases. The Institution has in place systems and procedures to ensure that information remains consistent and accurate throughout the databases and to enable the provision of staff services, such as the establishment of e-mail accounts and library membership.

Disclosure of data

Data will be processed in accordance with the provisions of the Act and will only be disclosed within the Institution to members of staff who need to know it in order to carry out their duties, or to others connected with the University for University-related activities or events. Data will only be disclosed to a third party outside the Institution in accordance with the Act. This may include future employers who require verification of your period of employment.

Use of IT facilities

The University of Suffolk reserves the right to exercise control over all activities relating to its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources. This monitoring may include access to personal data held and managed on the IT facilities and networks. The reasons for undertaking such monitoring include ensuring adherence to the University of Suffolk's Guidelines for Use of IT Facilities.

Information provided to the Higher Education Statistics Agency (HESA)

Some of the data held about you will be sent in a coded and anonymised form to HESA on an annual basis. From there it will be added to a database which is passed to central government departments and agencies to enable them to carry out their statutory functions under the Education Acts. It will also be used by HESA and other bodies for statistical analysis leading to publication and release of data to other approved users including academic researchers and unions. Please note that your name and contact details will not be made available to HESA.

Data retention

If you decide to leave, a permanent record of your period of employment at the University of Suffolk will be retained.

Your rights as a Data Subject under the Act

You have a number of rights relating to the personal data which the University of Suffolk holds about you. The main ones are as follows:

- To be given a copy of any data held, whether on a computer or in a manual file.
- To ask the University not to process any data held about you on the grounds that it might cause you substantial damage or distress.
- To ask the University not to use your personal data for the purposes of direct marketing, should this ever be undertaken by the University of Suffolk.

The University has a Subject Data Access Request Form which is available on the University of Suffolk website with instructions for completion. A fee of £10 is charged for each request made.

Your responsibilities as a Data User under the Act

You have three main responsibilities as a University of Suffolk employee with respect to the processing of personal data:

1. If you hold personal data in any form, whether on computer or in a manual file, as part of your job, this must be registered with your business unit in a form accessible by the Data Controller whose responsibility it is to ensure the Institution's data protection procedures are accurate and up-to-date. This includes any data that might be held by members of academic or academic-related staff for research purposes;

2. In dealing with personal data as part of your job, you must ensure that it is not shared with anyone other than individuals connected to University of Suffolk who need to know it in order to perform their work function. This covers both intentional disclosure and any disclosure that might happen by accident, for example through someone having oversight of your PC screen on which data is displayed. It is particularly important that personal details about members of staff or students are not given to anyone outside the Institution without prior consent of the individual concerned. If you are in any doubt, please do nothing until you have sought advice;

3. If you are a member of academic or academic-related staff, you are also responsible for ensuring that any students under your supervision who process personal data as part of their studies, for example in an undergraduate project or a postgraduate dissertation, conform to the requirements of the Act. Students who find themselves processing personal data as part of their studies are asked to contact their supervisor in the first instance; if you receive any such approaches please contact your line manager for advice.

Help and advice

You may seek help and advice about the Data Protection Act, and how it affects you both as a Data Subject and as a Data User, from your line manager in the first instance or from the Head of Management Information / Academic Registrar / Director of HR / Head of IT Services.

Appendix 4: Data Subject Access Request (SAR) Form for Staff

I, _____, wish to have access to data which the University of Suffolk has about me in the following categories: (Please tick as appropriate.)

- Employment references
- Disciplinary grievance and capability records
- Health and medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information: please list below

_____

_____

_____

_____

I understand that a fee of £10 per request will be payable. (Please make cheque payable to University of Suffolk.)

Signed _____

Dated _____

Appendix 5: Student data protection notice

The University of Suffolk has a notification under the Data Protection Act 1998 to hold relevant personal data about its students, for example, data about your admission, academic background, course registration, methods of payment and academic progress while at the University, together with data about your accommodation and that collected for the purposes of equal opportunities monitoring. This data is processed for various administrative, fee collection, academic, and health and safety purposes. It is processed in accordance with the provisions of the Act and is only disclosed within the Institution to members of staff who need to know it in order to carry out their duties or to others connected with the University for University-related activities or events. Where you provide a mobile telephone number, the University may use this number to contact you by text message with relevant, University-related information.

Specific disclosure of data

If you are involved in an emergency situation which results in you being hospitalised, the University of Suffolk may provide your emergency contact details to the relevant authorities dealing with the emergency, e.g. police, fire brigade or ambulance.

Your details are shared with the Students' Union to provide you with access to the Union and its services, as well as to enable the University to fulfil its legal obligation to support the operation of a fair and democratic Students' Union.

Under the provisions of the Representation of the People Act 2000, the University of Suffolk provides personal information about you to Electoral Registration Officers for the purposes of maintaining registers of parliamentary and local government electors. Personal data about you may also be provided to the relevant local authority in relation to the collection of Council Tax. Should you incur any debt (tax-related or not) while registered as a student at the University of Suffolk, it is likely the Institution will comply with external requests to disclose personal information about you in relation to the collection of the debt.

If you are registered at the University of Suffolk and are taught at a partner college by formal arrangement, your data may be disclosed to that institution as appropriate to enable them to carry out their duties with respect to your studies. In all other cases, data is only disclosed to a third party outside the Institution in accordance with the Act. This may include prospective employers who

require verification of your qualifications, or other educational establishments if, at the end of your time at the University, you decide to undertake studies elsewhere.

Use of IT facilities

The University reserves the right to exercise control over all activities relating to its IT facilities and networks, including monitoring of systems and electronic communications and access to external electronic resources. This monitoring may include access to personal data held and managed on the IT facilities and networks. The reasons for undertaking such monitoring include ensuring adherence to the University of Suffolk's Guidelines for Use of IT Facilities.

Information about you provided to the Higher Educations Statistics Agency (HESA) and Higher Education Funding Council for England (HEFCE)

Some of the data held about you is sent, in a coded and anonymised form, to HESA on an annual basis. From there it is added to a database which is passed to central government departments and agencies to enable them to carry out their statutory functions under the Education Acts. It is also used by HESA and other bodies for statistical analysis leading to publication and release of data to other approved users, including academic researchers and commercial bodies. Please note that your contact details are not made available to HESA; your name is not used or included in any statistical analysis; and precautions are taken to minimise the risk that you are able to be identified from the data. Neither statutory nor non-statutory users of the data supplied to HESA are able to use the data to contact you.

For individuals who are eligible to take part in the National Student Survey (NSS), which is organised by HEFCE, information about you may be supplied by the University of Suffolk to HEFCE or agents acting on its behalf. HEFCE's appointed agent may contact you directly to take part in a survey to provide feedback about the quality of programmes of study. HEFCE may also share this information with the Department of Health (for NHS-funded students). If you are contacted in connection with the NSS, you have the right to opt out from taking part in the survey at any stage.

Six months after you graduate, the University will contact you in relation to the Destinations of Leavers from Higher Education (DLHE) survey. As part of this process, your contact details may be passed on to HESA. Two and a half years later, there is the possibility that you may be contacted by HESA or agents acting on behalf of HESA, for a follow up survey, the Longitudinal (DLHE) Survey.

You will have the opportunity to object to these contacts if you wish. Further details about the surveys and what happens to the information that is collected can be obtained from the Infozone.

Data retention

When you leave, appropriate data is kept as a permanent record to enable the University, if necessary, to provide references on your behalf, or to maintain a record of your academic achievements. The data is transferred to the University's record of its past students to enable us to keep in touch with you after you leave.

Your rights as a Data Subject under the Act

You have a number of rights relating to the personal data which University of Suffolk holds about you. The main ones are as follows:

- To be given a copy of any data held, whether on a computer or in a manual file.
- To ask the University of Suffolk not to use your personal data for the purposes of direct marketing.

The University of Suffolk has established procedures for dealing with subject access requests which should be made using the appropriate form available on the University of Suffolk website. Please note that it is University policy to disclose examination marks to students and to make the contents of a student personal file, held in Academic Services, available to the student concerned. It is not necessary, therefore, to use the subject access provisions of the Act to obtain access to this data.

The University has a Subject Data Access Request (SAR) Form available on the University of Suffolk website which should be completed and submitted in accordance with instructions. A fee of £10 is charged for each request made.

The Infozone will be pleased to help with any queries you might have about any of your rights under the Act.

Your responsibilities as a Data User under the Act

It is unlikely that you will find yourself processing personal data as part of your studies at the University. However, if you do, perhaps as part of an undergraduate project or postgraduate dissertation, you will become a Data User under the terms of the Act and you will need to take certain steps to ensure that the University knows what you are doing and that your processing of data

conforms to the requirements of the Act. This does not apply to any personal data that you might hold for domestic or personal uses.

If you find yourself in this position, or are in any doubt, please see your Course Leader or Supervisor in the first instance.

Help and advice

You may seek help and advice about the Data Protection Act, and how it affects you both as a Data Subject and as a Data User, from the Infozone.

Appendix 6: Data Subject Access Request (SAR) Form for Students

I, _____ wish to have access to the data which the University of Suffolk currently has about me in the following categories either as part of an automated system or part of a relevant filing system: (Please tick as appropriate.)

- Academic marks or course work details
- Academic references
- Health and medical matters
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc.
- Other information: please list below

_____

_____

_____

_____

I understand that a fee of £10 per request is payable. (Please make cheque payable to University of Suffolk.)

Signed _____

Dated _____

Appendix 7: Staff data collection consent

Extract from the University of Suffolk Contract of Employment for all staff:

DATA PROTECTION

University of Suffolk employees are required to comply with the provisions of the Data Protection Act 1998 and with the University's Data Protection and Data Security Policy. By accepting this employment, you consent to the University processing personal data relating to you as necessary for the performance of your contract of employment and/or the conduct of the University's business. Further, you explicitly consent to the University processing any sensitive personal data relating to you, including but not limited to self-certificates, doctors' certificates, medical reports, details of trade union membership or details of criminal convictions as necessary for the performance of your contract of employment and/or the conduct of the University's business.

Appendix 8: Student data collection consent

Data Protection Summary from OASIS:

The University of Suffolk collects information about all students for various administrative, academic and health and safety reasons. Under the provisions of the Data Protection Act 1998, the University asks you to give your consent before we do this.

Since the University of Suffolk cannot operate effectively without processing information about you, you are required to sign the Declaration on the University of Suffolk enrolment form. If you do not do so the University may not be able to offer you a course place and may have to withdraw any offer already made.

The University of Suffolk may release your personal data to third parties including current or potential employers, examination bodies, government departments or agencies or as otherwise required by law. Some examples of these are listed below:

- Higher Education Statistics Agency – A statutory return for all Higher Education Institutions
- The University of Suffolk Students' Union – To enable membership of the Students' Union
- Potential Employers – To provide a reference in relation to a job application
- Current Employers – Where the employer is responsible for funding the course for a staff member, the University of Suffolk may confirm the status of the student on the course (current or withdrawn) and the results of any assessments taken
- Under the terms of The Registration of the People (England and Wales) Regulations 2001, part III, paragraph 23 relevant data may be shared with the local Electoral Registration Officer
- The Students Loans Company – to confirm attendance to enable payout of loan payments
- Cloud based applications/systems used by the University of Suffolk that comply with all relevant Data Protection and Security regulations. For example, www.gradintel.com, which is used to host each student's Higher Education Achievement Report (HEAR)

Extract from Student Enrolment Form:

Data Protection

You agree to the University of Suffolk processing your personal data contained within this online form and other data which may be obtained from you or other sources, including sensitive data where

applicable, whilst you are a student at the University of Suffolk and, where relevant, once you have ceased to be a student. You agree to the processing of such data for the purposes set out in the guidance found here.

Notification of personal data held by the University of Suffolk

This notice is served as part of the requirement of the Data Protection Act 1998. It sets out the types of personal data that the University currently holds about you or may hold about you once your enrolment has been processed and you have begun your studies. You have the right to request copies of most of the information we have about you.

We currently hold, or will hold where relevant, information in the following categories that requires your consent to process:

- Personal details that were provided by you on enrolment and application forms, including name, address, qualifications, next of kin.
- Details about student academic performance and expected results, references and recommendations and attendance.
- Details about student course fees and loans, applications for assistance from access and hardship funds, course registration, library and other equipment on loan.

We need your express consent to process any sensitive personal data that you may provide to us. This might include, for example, what you have told us about your racial or ethnic origin, physical or mental health, financial matters, or criminal record. Please note that the information we will have is only that which you will yourself have provided to us (or given permission for other bodies to provide to us).

Such information may be used for the following purposes:

- Checking suitability and fitness for course places
- Managing and maintaining a safe working environment
- Managing duties and obligations under various legislative requirements including the Disability Discrimination Act and the Race Relations (Amendment) Act
- Managing your time as a student

Appendix 9: Data protection staff briefing

All new staff to be given guidance during induction and updates provided at team meetings.

What does the Data Protection and Data Security Policy mean to you?

As a publically accountable body, the University of Suffolk is bound by the Data Protection Act (DPA) and is responsible for the protection of this type of information, termed 'sensitive data'. This means any personal information that can be specifically linked to an individual. The DPA covers data on current and former students and staff, potential students and staff, and members of the public. We therefore have to take reasonable measures to ensure that sensitive data is not put at risk of loss or theft. If the University is successfully challenged under the DPA, there is a very real possibility of a hefty fine as well as subsequent scrutiny from the legislators.

The DPA gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly. The University's obligations are:

- to notify the Information Commissioner that the University of Suffolk is processing information;
- to process personal information in accordance with the eight principles of the Act which make sure that personal information is:
    - Fairly and lawfully processed
    - Processed for limited purposes
    - Adequate, relevant and not excessive
    - Accurate and up to date
    - Not kept for longer than is necessary
    - Processed in line with the individual's rights
    - Secure
    - Not transferred to other countries without adequate protection;
- to answer subject access requests received from individuals. These may be staff, students or any individual who has an association with the University of Suffolk. They have important rights, including the right to find out what personal information is held on computer and most paper records.

What should you do?

Remote access has been facilitated so as a user you can access the University of Suffolk intranet and your files from any location. Therefore, there should be few reasons to transfer sensitive information away from your desk or access it outside of the University of Suffolk secure IT network. We do not recommend removing paperwork and storing information electronically on portable devices including laptops, memory sticks and disks. These are all vulnerable to loss or theft if left in cars, on public transport or in the home. Laptop and data loss from public sector organisations is commonly reported in the press and it would be regrettable if the University made the headlines for a data security breach. Additionally, the University is not insured for such losses and you may be open to the University of Suffolk Disciplinary Procedure. If you sometimes work from home or elsewhere offsite, you should only access sensitive data through the secure IT network.

Some of you will be presenting at conferences or meetings and will often take your presentation on a memory stick. This is normally not a risk as such data will be in the public domain when you present it so by definition is not sensitive. However, if you are dealing with sensitive information you must ensure you comply with the rules given below.

Rules

- Do not remove sets of sensitive information about staff, students or the public from your work location or from the secure IT network; e.g. names and addresses of students, examination grades, job application forms etc.
- Keep your user ID and password for the IT network secret and secure.
- When working offsite, always access your documents by logging on to the University of Suffolk network and accessing the VLE or shared ‘N drive’.
- Do not leave your laptop unlocked and unattended whilst logged on.
- Do not leave printed copies of sensitive data in plain view.
- Do not leave sensitive data on screen where others can see it.
- Do not disclose sensitive data to third parties without authorisation. If you are not sure how to handle a data request, contact the University of Suffolk Data Controller
- Do not copy sensitive data onto laptops, iPad or other mobile devices, e.g. flash drives, CD-ROMs, memory sticks. Even if your laptop/iPad is password protected, this is no barrier to a determined hacker.
- Always store data on the network ‘N drive’ so that it is backed up each night. If you store information on the local ‘C Drive’ it is not backed up and is vulnerable to theft.

- Never share your University of Suffolk password with colleagues because you may have different levels of access to restricted areas within the network related to your roles within the organisation.
- Anonymise data if using it with an audience who are not authorised for full disclosure. However, be aware that with small subject groups it is sometimes possible to identify individuals even if names are not used. This should not be allowed to happen.