NORWICH
UNIVERSITY
OF THE ARTS

Vice-Chancellor: Professor John Last

DATA PROTECTION POLICY

Academic Registrar

Approved by Senate: 30 January 2013

CONTENTS

1. Policy Statement

1.1 The University is committed to a policy of protecting the rights and freedoms of individuals by adhering to principles of the Data Protection Act 1998. These rights extend to staff, students, visitors to and agents of the University. It is necessary for the University to use personal data for management, administration and research but in doing so it will conform to this Policy as dictated by the Data Protection Act 1998.

2. The Principles of Data Protection Act 1998

2.1 There are eight principles put in place by the Data Protection Act 1998 to make sure that information is handled properly. They state that data must be:

1. fairly and lawfully processed;
2. processed for limited purposes;
3. adequate, relevant and not excessive;
4. accurate;
5. not kept for longer than is necessary;
6. processed in line with your rights;
7. secure; and,
8. not transferred to countries without adequate protection.

By law data controllers have to keep to these principles.

3. Definitions

3.1 Personal data

Data which relates to a living individual (known as a data subject) who can be identified from that data; or can be identified from that data and other information in the possession of the data controller. This also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. Examples of personal data would include personal details such as name, address, telephone number, email address or identification/student number.

3.2 Sensitive data

Information about a data subject which relates to the following: racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; health; sex life; criminal proceedings against the data subject or any criminal convictions. Sensitive data are subject to much stricter conditions of processing.

3.3 Processing

Any activity which involves obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including organisation, adaptation, alteration, retrieval, consultation, disclosure, dissemination, alignment, combination, blocking, erasure or destruction of the information or data.

3.4 Data Subject
A data subject is a living individual who is the subject of personal data held by an organisation.

3.5 Data Controller
The data controller is any person or organisation which determines the purposes for which and the manner in which any personal data are, or are to be, processed. Norwich University of the Arts is the data controller.

3.6 Data Processor
In relation to personal data the data processor is any person (other than an employee of the data controller) who processes the data on behalf of the data controller. Where this takes place the data controller retains full responsibility for the actions of the data processor.

3.7 Third Party
In relation to personal data a third party is any person other than the data subject, the data controller, or any data processor or other person authorised to process data for the data controller or processor. Family members, friends, government bodies and in certain circumstances the Police are all classed as third parties.

3.8 Information Commissioner

The Information Commissioner enforces and oversees the **Data Protection Act 1998 (DPA)** and the **Freedom of Information Act 2000 (FOI)**.

The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one. Under the Data Protection Act 1998 the Information Commissioner can:

- In certain circumstances serve an information notice and assess compliance with the Acts. This requires a data controller to provide the Commissioner with specified information within a certain time period, which will help him to assess compliance.

- Where there has been a breach, to serve an enforcement notice ordering compliance, where there is an ongoing breach of the Acts (which requires data controllers to take specified steps or to stop taking steps in order to comply with the law).

4. Notification

The Data Protection Act 1998 requires every data controller who is processing personal data to notify unless they are exempt. The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. The principal purpose of having notification and the public register is to permit to find out who is carrying out processing of personal data and other information about the processing, such as,

for what purposes the processing is carried out. The Act places obligations on data controllers in order to achieve transparency.

Anyone within the University who intends to process data should ensure that this is covered within the University's notification to the Information Commissioner. Guidance is available from the University's Data Protection Officer.

5. Data Processed by Norwich University of the Arts

5.1 Students

Data is collected at application. At enrolment where the student confirms their attendance on the course additional information is collected. A student file is set up and the following information will be collected and kept on file for the duration of the student's course:

- Personal data on application forms (through UCAS for undergraduate courses);
- Personal data collected through the enrolment form;
- Data collected for Student Support including sensitive data on health and disabilities;
- Data collected to confirm fees status and for applications for financial assistance;
- Confirmed student marks;
- Extensions to academic deadlines;
- Submissions for extenuating circumstances and supporting documentation;
- Medical notes;
- Correspondence to and from the student in respect of their academic studies.

5.2 Staff

Data is collected at application. Once the application is confirmed as successful, additional information is collected. A personnel file is set up and the following information will be collected and kept on file for the duration of the member of staff's employment plus six years:

- Personal data on application forms;
- Personal data collected through the New Employee Information Sheet;
- Personal data collected through the Change in Standing Data Forms;
- Sensitive data on the pre-employment Medical Enquiry Form;
- Sickness Absence Record;
- Forms relating to the member of staff's probationary period and review;
- Forms relating to the member of staff's performance review.

5.3 Credit card security

Credit card data is collected for a number of financial transactions at the University, including fee payments, gallery sales and degree show sales. The University Credit Card Security Policy sets out how the University controls the collection, transmission and storage of customer information and credit card data. The policy takes account of the standards set by the Payment Card Industry Security Standards (PCI SS) and the technical and operational

requirements of the PCI Data Security Standards (PCI DSS). All staff involved in credit card transactions are required to follow the policy and procedures laid down in Appendix 10 of this document.

6. Consent

All personal or sensitive data obtained by the University should be done so with the consent of the data subject. Consent is understood to be that the data subject has been informed that the data is being collected and agreed to the processing. The agreement should always being confirmed in writing with the data subject's signature particularly in the case of sensitive data. Consent cannot be inferred from non-response to communication.

The University obtains consent to process personal and sensitive data as follows:

6.1 Students

The University enrolment form includes a Data Protection statement which informs the student of the data will be processed by the University and details for what purposes it will be processed. It informs the student that by signing the enrolment form consent is being given to the processing of those data for the purposes detailed on the form. Students are requested to provide sensitive data (ethnicity and disability) on the enrolment form but the University cannot force the student to disclose this information.

All other personal data which is collected by the University on students eg. residence questionnaire is used for the purpose indicated on the form and for no other purpose. Where this is sensitive data this is not passed to any other area of the University without the University's explicit (written) consent eg. Disability Form.

6.2 Staff

The application form contains a Data Protection statement which informs the applicant of the data which will be processed by the University and details for what purposes it will be processed. Sensitive data is not requested on the application form and applicants are issued with a separate confidential return form where they are requested to tick a box indicating ethnic group, age group, gender, nationality and gender. The information provided is anonymous and is not circulated as part of the short-listing process.

Other forms collecting personal data includes a Data Protection statement which informs the member of staff that all or parts of the information on the form may be stored on computer files and manual files and used for the purpose of personnel and payroll administration and such use will be subject to the provisions of the Data Protection Act 1998. They inform staff that by signing the form consent is being given to the processing of those data for the purpose of personnel and payroll administration.

7. Security of data and responsibilities of staff

All staff should ensure that personal data is held securely and is not disclosed to any unauthorised third party (see **Disclosure**).

All personal data should be kept as follows:

- Paper files
  - In a locked storage system;
  - In a lockable room with controlled access.

- Computer files
  - Password protected, encrypted or where possible, removal of personal details;
  - Kept on disk and securely stored;
  - Ensure computer screens are not visible and passwords are kept confidential.

All staff who process personal data have a responsibility to ensure that data is stored and disposed of securely. Manual records containing personal data must be shredded either internally or through the University's shredding service.

This policy applies to all staff and students who process personal data and includes any processing undertaken off the University's premises. Particular care should be taken when processing is undertaken away from the University and here possible this should be avoided.

Data is only accessible to those who have a legitimate interest in seeing the data. Data subjects have the right to apply to the court for compensation if damage or distress has been suffered because of loss, destruction or unauthorised disclosure to a third party.

8. Disclosure

Under the Data Protection Act (1998), Norwich University of the Arts must not disclose data to unauthorised third parties. A 'third party' includes family members, friends and external agencies.

The University may legitimately disclose information where the following conditions apply:

- The individual has given explicit consent for the information to be released to a named third party;
- Where the disclosure is in the legitimate interests of the University eg. disclosure of staff or student information to certain other members of staff in order to allow the University to function;
- Statutory obligations of the University to provide information to external agencies including HESA and HESES returns, ethnic minority and disability monitoring;
- Where disclosure is required for performance of a contract (eg. informing the student's LEA or sponsor of course changes/withdrawal).

The Act also permits certain disclosures without consent as long as the information is required for one of the following purposes:

(i) To safeguard national security;
(ii) For prevention or detection of crime including the apprehension or prosecution of offenders;
(iii) Discharge of regulatory functions (including health, safety and welfare of persons at work);
(iv) Where disclosure is needed in life and death situations for the safety and well being of the individual as determined by the University;
(v) To prevent serious harm to a third party.

With the exception of (iii) it is necessary that the University's Data Protection Officer (Academic Registrar) be informed in order that appropriate procedures are followed.

In addition, the University also discloses information for the following reasons:

(vi) References for current or prospective employers or educational institutions;
(vii) Progress reports for student sponsors as set out in a sponsorship contract;
(viii) Publication of names of graduating students in the degree ceremony graduation programme.

Where a member of staff is requested to write a reference for a member of staff or student it is advised that every precaution is taken to ensure that the information is not being released without the individuals' consent or knowledge to a third party. In most cases this can be ensured by requesting a copy of the form which includes the individual's consent to approach the University for a reference. Further information can be found under **References**

Students are given the opportunity to opt out of (viii) and in addition, they may notify the Academic Registrar in writing at any time up to 7 days before Graduation.

Disclosure to the Police

It is not compulsory to disclose information to the Police except where a Court of Order is served requiring information.

The Data Protection Act does allow the University to release some information without the consent of the individual in certain circumstances. Any requests for information should be directed to the Data Protection Officer in these circumstances and should be writing unless it is felt that it is a life and death situation.

If the information is to be passed on verbally the name, telephone number and number of the investigating officer is needed in order that they can be called back with the information.

Disclosure of students in receipt of learning support

Explicit consent must be given by students to release this information as this is sensitive information. A student must be advised of who would require this information in order for the University to perform its job and the student must sign to confirm their consent to this information being released. If the student does not wish for this information to be released they should be advised that this may limit the University in providing the support and the student should be asked to put their refusal in writing.

9. Disclosing personal data overseas

The Act contains specific provisions with regard to the transfer or personal data outside of the EEA. This is set out in the eighth Data Protection principle. Data must not be transferred to any country that lies outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA comprises the member states of the EU as follows:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK:

plus Norway, Iceland and Liechtenstein.

However, data can be transferred with the consent of the data subject and it is advisable to seek consent at the point of collection where it is known that there will be a need or wish to transfer data overseas.

In line with the Act, personal data should only be disclosed to countries outside the EEA if certain conditions are met as follows:

- There is explicit consent for this disclosure (in writing)
- The disclosure is required for performance of a contract
- Disclosure is necessary for the purposes of legal proceedings (where the University is taking legal action)

This applies to University activities in respect of individual students and where the course operates and exchange agreement with an institution in a country outside of the EEA.

10. Retention and Disposal of data

Once a member of staff or student has left the University it is not necessary to retain all information held on them.

- **Students**
  Student files are kept for a period of six years after a student has left the University. After this period all student records are confidentially destroyed.

The University keeps a permanent record of the student's enrolment, course and academic progression.

- **Staff**
  Please refer to **Appendix 7: Retention Schedule For Staff Records**

11. Right of Access to Data

All persons about whom the University holds data (data subject) may request to see the data held on them (staff and students). This is known as a Subject Access Request. Anyone who makes a Subject Access Request **must** be referred to the University's Data Protection Officer who will coordinate the request for data and contacts the relevant offices. Requests must be made formally to the University in writing using the application form (see: Subject Access Request Procedure). A fee may be charged for this service and the University must respond to any formal request within the relevant timescale. Please refer to the Subject Access Request Procedure set out in Appendix 2.

12. Use of Personal Data in Academic Research

Personal data collected only for the purposes of academic research (the work of staff and students) must be processed in compliance with the Data Protection Act 1998.

The 1998 Act provides certain exemptions for **research** purposes including statistical and historical purposes. If the purpose of the research processing is not to support measures or decisions targeted at particular individuals AND it does not cause substantial distress or damage to the data subject then the following exemptions may be applied:

- that personal data can be processed for purposes other than for which they were originally obtained (exemption for second data protection principle);
- that data can be held indefinitely (exemption from fifth data protection principle);
- that personal data are exempt from data subject access rights where the data are processed for research purposes and the results are anonymised (exemption from part of the sixth data protection principle relating to access to personal data).

This exemption does not give blanket exemption from all of the Data Protection principles. Researchers who wish to use personal data should note that most of the Data Protection principles still apply including the requirement to keep data secure.

On any occasion where data are provided for research purposes and assessment of the legality of the processing should be undertaken. Periodic monitoring should also be carried out to ensure adequate compliance.

Clear guidance as to why the data is being collected and the purposes for which it will be used in research to data subject whose personal data will be used in research. Where the data collected includes sensitive data extreme care should be taken to ensure that explicit consent is given and that the data are held securely and confidentially so as to ensure against unlawful disclosure.

Researchers should ensure that the results of the research are anonymised when published and that no information is published that would allow individuals to be identified. Results of research can be published on the web but where personal data is included the explicit consent of the individual must be gained. Please refer to section 9

13. Disclosing personal data overseas

The Act contains specific provisions with regard to the transfer or personal data outside of the EEA. This is set out in the eighth Data Protection principle. Data must not be transferred to any country that lies outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA comprises the twenty five member states of the EU as follows:

Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, UK:

plus Norway, Iceland and Liechtenstein.

However, data can be transferred with the consent of the data subject and it is advisable to seek consent at the point of collection where it is known that there will be a need or wish to transfer data overseas.

In line with the Act, personal data should only be disclosed to countries outside the EEA if certain conditions are met as follows:

- There is explicit consent for this disclosure (in writing)
- The disclosure is required for performance of a contract
- Disclosure is necessary for the purposes of legal proceedings (where the University is taking legal action)

This applies to University activities in respect of individual students and where the course operates and exchange agreement with an institution in a country outside of the EEA.

14. References

Personal references (and other personal data) are exempt from subject access requests

This exemption from disclosure does not apply to the individual or organisation that receives the reference and subject access can be requested.

Every precaution is to be taken to ensure that when supplying a reference the information is not being released without the individuals' consent or knowledge to a third party. In most cases this can be ensured by requesting a copy of the form which includes the individual's consent to approach the University for a reference.

Before providing the reference it is necessary to ensure that:

- the information is factually correct**;**
- the minimum amount of data is disclosed;
- sensitive data is not disclosed (details of health or absences from the University) unless there is explicit (written) consent from the individual for this information to be released;
- Opinions about the individual's suitability should be avoided but if necessary are those that could be justified if necessary.

It is essential that the identity of the organisation requesting the reference is confirmed. Consequently, it is not recommended to provide a verbal reference by telephone but where a reference is requested at short notice it may be necessary. In such cases for security the caller must be rung back via a central switchboard number.

The University would normally expect a reference request to be in writing on appropriate headed paper of the company. Ideally the company should provide a copy of the section where the member of staff or student has given their consent to contact the University. A response should only be made to requests made by email where the identity of the organisation/person requesting the reference can be verified.

It is possible to refuse to provide a reference on the grounds that it is not possible to verify the identity of the organisation but care should be taken as this must not be mistaken for refusal to provide a reference for negative reasons.

APPENDIX 1: GUIDE TO UNIVERSITY PUBLICITY

Personal data

Personal information of staff and/or students can only be used in University publicity where consent has been given by the individual for that purpose (eg. where the individual has given consent for the personal information to be published in a specific publication and not where the individual has given consent only for the personal information to be taken). University publicity would include information published on the University's internet site or in any other publication which is likely to be seen externally (eg. prospectus, annual report). Personal information would include name or personal email address or other information where an individual might be identified.

Where a member of staff is preparing a document for internal consideration but which may, at a subsequent date, be externally distributed (eg. course evaluation document), care should be taken to avoid identifying people by name without their permission.

Photographs

Photographs for University publicity where individuals (staff and/or students) **cannot** be readily identified may be used without obtaining consent (eg. graduation photographs)

Photographs of individual members of staff and/or students (or small groups where individuals can be identified) can only be used in University publicity where consent has been given by the individual for that purpose (eg. where the individual has given consent for the photograph to be published in a specific publication and not where the individual has given consent only for the photograph to be taken).

Please refer to Section 9 Disclosing personal data overseas for further guidance about the transfer of data used in the University's publicity.

APPENDIX 2: SUBJECT ACCESS REQUESTS

The Data Protection Act 1998 gives individuals (data subjects) the right to access personal data that the University holds on them. This right of access extends to all information held on an individual (staff and students) and includes personnel files, student record files, databases, interview notes and emails referring to the individual. In order to view their files an individual needs to make a "Subject Access Request" for which the University can charge a fee.

A Subject Access Request must be made as follows:

- the request must be in writing
- information must be provided to prove who they are (in order to avoid against unauthorised disclosure)
- to provide information to assist the University to locate the specific information required

The University must respond to a Subject Access Request within 40 days as follows:

- information on whether or not the personal data are processed
- a description of the data, purposes and recipients
- a copy of the data
- an explanation of any codes/jargon contained within the data.

Procedure for submitting a Subject Access Request

1. The request must be made in writing to the University's Data Protection Officer (Academic Registrar);

2. Documented evidence of identity must be included with the request (eg. driving licence, passport);

3. Details of the information which is wanted to be accessed such as where this information is held. It is not necessary to include an explanation of why the information is required;

4. The University is permitted by the Act to charge an administration fee. In most straightforward cases this fee will be waived. However, where the Data Protection Officer believes that the administration involved in responding to a Subject Access Request is significant the University will charge the fee to cover costs;

5. The Act requires the University to respond to Access Requests within 40 days. In cases where gathering of information is likely to take longer than this period or where the Data Protection Officer requires more specific information on the data required from the data subject, the individual will be informed in writing;

6. In accordance with the Data Protection Act 1998, the University is not permitted to release information held about individuals without their consent. Where information held on the individual making the subject access request also contains information related to a third party the University will attempt to anonymise the information or if necessary secure the consent of the third party before releasing the information. Where neither is possible, the University may decide not to release this information to the individual.

Exemptions

There are certain situations where the University may not be obliged to release information in response to a Subject Access Request.

Examples include:

- Data containing information relating to a third party for which consent to release the information cannot be obtained;
- Assessment notes although assessors' comments MUST be released (see Assessment);
- Information relating to legal proceedings being taken by the University against an individual.

All individuals should be referred to the University's Data Protection Officer (Academic Registrar) when they wish to make a Subject Access Request.

APPENDIX 3:DISCLOSURE OF STUDENT INFORMATION AND USE OF DATA

Norwich University of the Arts collects and holds information on students in electronic and/or paper form in order to manage a number of University activities including enrolment, assessment and graduation as well as providing comprehensive student services including student support, disability support, international student support, IT and library services and careers advice.

Disclosure of student information to third parties

Under the Data Protection Act (1998), Norwich University of the Arts must not disclose data on students to unauthorised third parties. A 'third party' includes family members, friends and external agencies.

The University may legitimately disclose information where the following conditions apply:

- The individual has given explicit consent for the information to be released to a named third party
- Where the disclosure is in the legitimate interests of the University eg. disclose of staff or student information to certain other members of staff in order to allow the University to function
- Statutory obligations of the University to provide information to external agencies including HESA and HESES returns, ethnic minority and disability monitoring
- Where disclosure is required for performance of a contract (eg. informing the student's LEA or sponsor of course changes/withdrawal)

The Act also permits certain disclosures without consent as long as the information is required for one of the following purposes:

(i) To safeguard national security

(ii) For prevention or detection of crime including the apprehension or prosecution of offenders

(iii) Discharge of regulatory functions (including health, safety and welfare of persons at work)

(iv) Where disclosure is needed in life and death situations for the safety and well being of the individual as determined by the University.

(v) To prevent serious harm to a third party

With the exception of (iii) it is necessary that the University's Data Protection Officer (Academic Registrar) be informed in order that appropriate procedures are followed.

In addition, the University also discloses information for the following reasons:

(vi) References for current or prospective employers or educational institutions;

(vii) Progress reports for student sponsors as set out in a sponsorship contract;

(viii) Publication of names of graduating students in the degree ceremony graduation programme.

Students are given the opportunity to opt out of (viii) and in addition, they may notify the Academic Registrar in writing at any time up to 7 days before Graduation.

Requests to release information

Students may be required by various agencies to provide evidence of their status as student at Norwich University of the Arts. This may be for reasons of discounted student access to leisure facilities. Students may also require the University to provide information on their studies over and above that which is would normally provide for the reasons indicated in points (vi) and (vii). In these situations the University will require students to complete a Consent to release student information form which are available from the course office, Student Administration and Support and the intranet.

Use of student information within the University

Norwich University of the Arts retains all student information in a central filing system held by Academic Registry. Information on disability and support needs is held by Student Support. The information held includes all details provided at application and enrolment and copies of all written communications to and from the student. All files are kept in a secure and confidential filing system.

The information on files is not shared with other offices within the University unless there is a legitimate interest held by that office to have access to information. For example, information regarding medical conditions should be held on a student's file in case of emergency. If a student requires support for this condition then it would be legitimate for this information to be passed to the course office so that the necessary support is in place at all times. However, if there are no support requirements then it would not be necessary to pass on this information. This applies to other categories of data including disabilities. As a result duplicate copies of some information will be held at course level.

Students are asked to disclose medical conditions and disabilities prior to enrolment so that the University can support students appropriately.

The University tries to ensure that the information it holds is accurate and up-to-date. It must, however, rely on students to inform the appropriate office of any changes to personal data such as name or address. All changes should be made through the University's Registry by completing the appropriate form available from course administration offices or the intranet.

Disposal of student records

Student files are kept for a period of six years after a student has left the University. After this period all student records are confidentially destroyed.

The University keeps a permanent record of the student's enrolment, course and academic progression.

APPENDIX 4: ASSESSMENT

The rights of individuals to see information held on them by the University extends to documentation collated as part of the University's assessment processes:

Internal Assessors and External Examiners comments

Students are entitled to see comments made by assessors and examiners at assessment. Where these comments are made on an assessment script and where the script is not made available the course, the student is entitled to have a copy of all comments reproduced onto a separate form. Courses are advised to ask assessors and examiners to make comments on separate forms (where relevant). The comments must be given to students in "intelligible form". Where an assessor's or examiner's handwriting is illegible the comments must be reproduced in a clear form.

Courses should provide guidance to assessors and examiners in respect of this student entitlement and that any comments made as part of the assessment process can be justified and evidenced. Any related comments made by email or letter will be included in this access. There is no requirement to keep informal notes once a mark has been agreed and confirmed and that formal assessment record is kept. Informal notes should be disposed of securely.

Minutes of Course Assessment Boards/Final Award Boards/MA Assessment and Award Boards

Students are entitled to see the notes of meetings at which they are discussed although they are only entitled to see the notes specifically relating to them and/or agreement of their mark. Where a student is not discussed by name but by other identifiable source, the student is entitled to see the record of this.

It is essential that when a student is shown a record of an Assessment Board or Award Board meeting that any references to other individuals are anonymised.

The University can only consider refusing to provide this information only where this information could not be disclosed without additionally disclosing data about a third party without their consent.

Where an opinion of an Assessor or Examiner has been recorded in the minutes as part of the Board's discussion it is likely that such opinions and comments will have to be disclosed and therefore confidentiality cannot be guaranteed (see guidance above)

This includes the Resubmission Board

Extenuating Circumstances Panel

Students are entitled to see the notes of meetings at which they are discussed although they are only entitled to see the notes specifically relating to them. Where a student is not discussed by name but by other identifiable source, the student is entitled to see the record of this.

It is essential that when a student is shown a record of an Extenuating Circumstances Panel meeting that any references to other individuals are anonymised.

The University can only consider refusing to provide this information only where this information could not be disclosed without additionally disclosing data about a third party without their consent.

Publication of results

All assessment marks are regarded as personal data and must not be disclosed to third parties without the student's consent. Consequently, the University does not 'publish' marks on notice boards or at Graduation. If results are provided verbally in feedback sessions this must be done in such a way as to ensure confidentiality. At final award marks are provided in a sealed envelope collected by the student on production of a valid student card.

Requests made by students to see their results must be responded to within 5 months or 40 working days whichever is the sooner. This right extends to all students including those who owe money to the University and assessment marks can no longer be withheld.

Results must not be verbally disclosed over the telephone.

Alternative assessment procedures

Where alternative assessment arrangements have been put in place in order to support a student it is necessary that every care is taken in order to ensure these arrangements remain undisclosed. Where this is not possible (eg. in group sessions), the student needs to be advised of the need for disclosure in order for the support to be put in place and to gain the student's explicit consent for disclosure. If the student refuses disclosure then it will be necessary to advise them that the amount of support available might be restricted. Continued refusal to disclose must be respected at all times.

External examiners details

The University holds personal data on external examiners and external advisers. On appointment an external examiner or adviser should be informed for what purpose information held on them by the University will be used (eg. payment) and that their details will be held securely and will not be disclosed to a third party without their consent.

External examiners and advisors should be advised that any formal record retained by the University of comments or opinions expressed by them may be liable to a Subject Access Request by staff or students. External examiner reports will be published to staff and students on the University intranet. Likewise External examiners or advisors have the right to make a Subject Access Request regarding information held on them by the University including details on appointments and comments made by staff.

APPENDIX 5: HOW TO DEAL WITH REQUESTS FOR INFORMATION

Status of an individual

If an enquiry is received (verbal or written) as to whether a named individual is a member of staff or a student of the University it should be asked for what reason the information is required.

If there is no consent to disclose this information from the named individual and the reason is not one of those listed where consent is not required, this information should not be released. Confirmation of an individual's status at the University may constitute unauthorised disclosure and could be challenged

Disclosure of an individual's status at the University is not covered by the application or enrolment forms

Internal verbal requests for information on an individual

Information on an individual can only disclosed to colleagues if they have a 'legitimate interest' in the data concerned. Legitimate interest is not defined in the Act so it is necessary to make an assessment of each case. As a rule consideration should be given as to whether the information is necessary for them to do their job and what level of detail is required.

If this is a verbal request, the identity of the colleague should be confirmed. Care should be taken when disclosing information over the phone if the office is shared or is an environment where individuals can be overheard. If the identity of the member of staff cannot be confirmed they should be asked to put the request in writing with an indication of what the information would be used for.

External verbal requests for information on an individual

As a rule disclosures to external bodies should not be made over the phone.

Enquirers should be asked to put their request in writing. This also allows time to see if the body has a legitimate interest and to obtain consent for the disclosure by the individual in question.

Correspondence between all parties should be in writing.

If the situation requires disclosure over the phone due to time constraints and disclosure is permitted (eg. to a permitted external body such as UCAS or an LEA) identifying data should be requested: name, address etc along with the name and number of the organisation in order to call back with the information even if the caller is identifiable. The University must take every precaution to ensure that personal or sensitive data is not disclosed to an unauthorised third party.

What to do if a caller asks who deals with a particular area of work
If a caller needs to speak with someone who deals with a particular area of work or if is wrongly put through to a member of staff and needs to be redirected the caller should be advised of the appropriate member of staff by reference to the individual's job title and not be name (eg. you need to speak with the Academic Registrar) and give them the general University number. As a rule the name and/or direct dial number of a staff or student should not be given to a caller without their permission

What to do if a caller asks to leave a message for a student or a member of staff
As a rule the University should not take messages for students. However, Reception should ask for the name of the course only and direct the call.

Without confirming whether or not a student is on a course, the caller should be asked what the nature of the message is. If it is an emergency, you should take their name and number and inform the Academic Registrar. If it is a general message the caller should be advised that the University cannot take messages for students. If the situation becomes difficult and if it is felt necessary to take the message the caller should be advised that the message will be passed on **if** the person is a student or member of staff at the University.

No confirmation should be given if you are asked whether someone is a member of staff or a student at the University.

Disclosure to parents (student information)
Parents are classed as a third party and therefore information on a student must not be disclosed even of they are paying the student's fees.

In an emergency the University would contact a student's next of kin (which is very often a parent). In these cases the Academic Registrar must be informed before contacting a parent.

Discussion with parents about University procedures eg. how graduation is undertaken is acceptable. The explanation must not relate to an individual's case but refer only to University-wide processes.

Home addresses, telephone numbers or email addresses
Personal/home numbers or email addresses of staff or students must not be disclosed to third parties unless there is explicit (written) consent from the individual.

A caller may be advised that the request can be passed to the staff or student if they are at the University.

For work contact details you should advise a caller of the person's job title and give the University's telephone number. University email addresses should not normally be disclosed without the permission of the member of staff and instead the generic University email addresses for course and support areas should be used. This will help to minimise direct marketing from external agencies.

APPENDIX 6: RECORDS MANAGEMENT

The University recognizes that the efficient management of its records is necessary, to support its core functions, to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. This document provides the policy framework through which this effective management can be achieved and audited.

The following principles are based on the JISC 'Model Records Management Policy for HE and Fe Institutions', July 2003.

1. Scope of the policy

1.1 These principles apply to all records created, received or maintained by staff of the University in the course of carrying out their institutional functions. Records and documentation created in the course of research, whether internally or externally-funded, are also subject to contractual record-keeping requirements.

1.2 Records are defined as all those documents, which facilitate the business carried out by the University and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including process for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

1.4 A small percentage of the University's records will be selected for permanent preservation as part of the University's archives, for historical research and as an enduring record of the conduct of business.

2. Responsibilities

2.1 The University has a corporate responsibility to maintain its records and Record keeping systems in accordance with the regulatory environment. The senior member of staff with overall responsibility for records management is the Academic Registrar.

2.2 The Academic Registrar is responsible, in consultation with colleagues on the Strategic Management Group (SMG) for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.

2.3 Individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the University's records management guidelines

2.4 Adherence to the University's records management procedures will in turn facilitate compliance not only with information-related legislation (specifically FoI

2000 and DPA 1998) but also with any other legislation or regulations (including audit, equal opportunities and research ethics) affecting the University.

3. Guidance

Guidance on the procedures necessary to comply with this Policy is available from the Academic Registrar. This guidance covers:

- records creation;
- business classification (for filing schemes);
- retention periods for records;
- storage options for records;
- destruction options for records;
- archival records: selection and management;
- external codes of practice and relevant legislation;

APPENDIX 7:RETENTION SCHEDULE FOR STAFF RECORDS

Type of data	Held by	Retention period
Employee Contract Management		
Records documenting an employee's initial application for employment with the University	HR Department	Termination of employment plus 6 years
Records documenting an employee's contract(s) of employment with the University	HR Department	Termination of employment plus 6 years
Records documenting disciplinary proceedings against an employee, where employment continues	HR Department	Closure of case plus 6 years
Records documenting grievances raised by an employee which relate directly to his/her own contract of employment, the University's response, action taken and outcome	HR Department	Closure of case plus 6 years
Records relating to the administration of an employee's contractual holiday entitlement	Finance	Current year plus 1 year
Records documenting an employee's absence due to sickness	HR Department	Termination of employment plus 6 years
Records documenting the authorization and administration of special leave, e.g. compassionate leave, study leave	HR Department	Termination of employment plus 6 years
Records documenting the authorization and administration of statutory leave entitlements, e.g. parental leave	HR Department	Termination of employment plus 6 years
Records documenting entitlements to, and calculations of, Statutory Maternity Pay	HR Department Finance	Termination of employment plus 6 years
Records containing an employee's basic personal details (e.g. address, next of kin, emergency contacts)	HR Department	While current
Records documenting an employee's termination of employment by voluntary resignation, redundancy, retirement (including on medical grounds) or dismissal	HR Department	Termination of employment plus 6 years
Recruitment		

Type of data	Held by	Retention period
Records documenting the advertising of vacancies	HR Department	Completion of appointment plus 1 year
Application form and application details for unsuccessful applicants	HR Department	Completion of appointment plus 6 months
Records containing summary statistical information about job applicants, e.g. ethnicity/gender analyses	HR Department	Completion of appointment plus 1 year
Records containing management analyses of recruitment effectiveness, e.g. use of advertising media	HR Department	Completion of appointment plus 1 year
Records documenting the handling of unsolicited applications for employment	HR Department	Not retained

APPENDIX 8: STUDENT RECORDS MANAGEMENT

Procedures for staff in storing and processing student records.
In order for the University to function efficiently a formal student record (in paper form) is held in the course area and centrally in Academic Registry and Student Support. In addition to the student record, information on students is also held electronically on the student record system. All information held on students must be kept confidential. The information held on the student file must not be transferred between areas unless it is necessary for the University to function.

Example of where student information is transferred between areas:

- Academic Registry inform Finance of a student's fee status

In some instances duplicate information is held at course level and centrally. This is where the information is relevant to both functions of the University.

Information that is not held on the student file
Some information is not held on the student file. This would be where a student disclosed information to a designated individual only or where the information disclosed is not relevant to the day-to-day functioning of the University:

Examples of where student information is not held on the student file:

- Student submission made for Extenuating Circumstances
- Submissions made in the case of a student appeal

In such cases this information is stored separately in the Academic Registry office.

Security procedures
In order to ensure the security of all information held by the University and to assist in the management of student records the following procedures are followed:

- Paper records are stored securely in a lockable cabinet in a lockable room to which access is restricted and controlled. A designated member of staff should hold the key with back up in that person's absence;
- Electronic student records containing personal and/or sensitive* data should, wherever possible, be kept to a minimum. Databases of student information including the University's Student Record System should be password protected. Copies of letter to students that are stored electronically must be stored on the University server or stored in paper form on the student file;
- Sending email containing student data should be avoided. Where an email is sent or received copies of the email should be deleted (inbox, sent items, deleted items). Sensitive data* must not be sent via email;
- Wherever possible, correspondence should not be sent where reference is made to more than one individual where that information needs to be stored on the student file. Where a Subject Access Request is made it would be necessary to anonymise all other forms of the document.

Any other information held outside of the student file (eg. PDPs held by academic tutors) should be stored securely in line with Data Protection procedures

Student Records Management in course areas

Student files should be stored securely in a lockable cabinet, in a lockable room with controlled access;

Courses should avoid holding information outside of the student file. Where this is impossible (eg. tutor's notes, PDPs), the same precautions in respect of storage and security apply. Reference should be made to the Data Protection policy regarding security.

Students need to be informed of all information which is being held on them, what it is used for, where it will be stored and to whom it might be disclosed. This information should be included in the Course Guide given to students at the start of their course. A list of all information held at course level should be kept so that files and information can be located efficiently. This is particularly important should a Subject Access Request be made.

Student Records Management in Academic Registry and Student Support (centrally)

Student files should be stored securely in a lockable cabinet, in a lockable room with controlled access.

Where it is not appropriate to store information on the student files (eg. submission of extenuating circumstances, student appeals and complaints), these will be kept in a separate file in the Academic Registrar's office.

In some circumstances it will be necessary to have duplicate information on the central and course area student file such as letters regarding study.

Copies of documentation on student files should not be given to individuals where there is no student file and any correspondence sent to individuals which makes personal reference to students should not be retained by the individual but should be destroyed once the necessary actions have taken place.

Where personal and/or sensitive data is collected by centralised support services an appropriate Data Protection statement must be included on the form to inform the student of why the information is being collected and for what purpose it will be used.

Student files should be archived after graduation in a secure area. The student file will be retained for a period of six years after which it will be destroyed. The University retains a record of the student's attendance, progression and final award. Files relating to appeals and complaints will be kept for a period of eight years.

APPENDIX 9:STUDENT CONSENT TO RELEASE INFORMATION PRO FORMA

STUDENT CONSENT TO RELEASE INFORMATION

I (name)_____a student in year__studying (course)_____ at the Norwich University of the Arts request the University to release the following information:

Please tick the appropriate box and complete the details as requested

□ To provide confirmation that I am a student studying at Norwich University of the Arts with the start and expected completion dates of my course to:

Name of company_____
Address of company _____
_____
_____

or

□ To provide confirmation as above **only** upon receipt of a formal request for this information from the following organisations:

Name of company 1_____
Name of company 2_____
Name of company 3_____

Signed_____Date_____

APPENDIX 10: CREDIT CARD SECURITY POLICY

1. INTRODUCTION

The purpose of this policy is to control the transmission and storage of customer information and data received in respect of processing receipts by credit or debit card.

This policy considers how the University obtains the customer information and data and how it is transmitted, processed, and stored.

Note: wherever a statement in this policy refers to 'Card', the statement applies to credit, debit, charge, and procurement cards, unless specifically stated otherwise.

2. REGULATORY BACKGROUND

Payment Card Industry Security Standards (PCI SS)
PCI Security Standards Council (PCI SSC)

The PCI Security Standards Council was founded by American Express, MasterCard Worldwide, and Visa Inc (amongst others). Participating organisations include merchants, payment card issuing banks, processors, developers and other vendors. It is a global open body formed to develop, enhance, disseminate, and assist with the understanding of security standards for payment account security. The Council maintains, evolves, and promotes the PCI security standards.

PCI Data Security Standards (PCI DSS)

PCI Security Standards are technical and operational requirements set by the PCI SSC to protect cardholder data. The standards apply to all organisations that store, process or transmit cardholder data. The Council is responsible for managing the security standards, while compliance with the PCI DSS is enforced by the founding members of the Council.

The PCI DSS applies to all entities that store, process and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. All Merchants who accept or process payment cards must comply with the PCI DSS.

MasterCard and Visa can impose substantial penalties for non-compliance with the PCI DSS regulations, with further penalties for any actual data compromise. As a final resort, the Merchant can be refused permission to process card data.

3. SCOPE

The main areas covered by this policy are:

- Receiving card data
- Transmitting card data
- Processing card data
- Storing card data

4. KEY CONTROLS

4.1 Receiving and transmitting card data

Card data should be received by appropriate methods only; preferably using face-to-face (chip & pin) transactions, where the customer is present and able to enter their card details directly into the card terminal; or via the online payments system.

Receiving card payments where the customer is not present is discouraged, but if it is necessary, the preferred method is to receive the card details by phone and enter them immediately into the card terminal.

Card details must never be sent by email or by other electronic method, or be entered into any online payment system other than that approved by the University.

Where personal card data has to be transmitted (from order taking / receiving location to card processing location), the card data must be recorded on NUA card authorisation forms (see appendix 1) and the forms must be kept secure at all stages of the transmission. Do not write down customer card details *anywhere other than on the 'card authorisation form'.*

Card authorisation forms must be hand delivered to Finance, do not transmit these via email or any other electronic method, or send the forms by internal or external post.

Where card data is received by post, the details should be immediately transferred to a card authorisation form, and removed from the posted document and destroyed.

4.2 Processing card data

Where the customer is present and the order taker or sales person has a card terminal, it is essential that customers enter their PIN (Personal Identification Number) into the card terminal unobserved. The customer's PIN or other card details must not be written down, electronically copied, or otherwise obtained or recorded.

Where face to face or over the phone transactions are not possible and card authorisation forms are used instead, these should be hand delivered to Finance as soon as possible who in turn should process the payment as soon as possible.

4.3 Processing card authorisation forms through the card terminal

Upon receipt of the card authorisation form(s) they should be checked for completeness and where possible the card transactions should be processed immediately through the card terminal by the card processor.

4.4 Incomplete Card Authorisation Forms

Where the card authorisation form is not complete, the originator should be contacted for the missing detail. Finance staff will refer back to the originating department for the required information.

4.5 Failed card terminal processing

Where the card terminal transaction fails to complete successfully and the transaction has been input from a Card Authorisation form, Finance staff contact the cardholder to inform him/her that the transaction has failed.

4.6 Storing card data

It is important that card data is treated as confidential and kept secure at all times.

Card authorisation forms that are awaiting processing should be stored in locked cabinets in rooms with restricted access to authorised personnel at all times.

Sensitive card data must never be retained after being used for processing.

All records of card security details or authentication data must be destroyed. The bottom of the card authorisation form, where such card details are recorded, must be cut off and shredded or destroyed by other means.

No track data (card electronic data) must be stored.

The rest of the card authorisation form, and till rolls supporting card transactions, can be stored after processing, as long as they are held in locked cabinets in areas with access restricted to authorised personnel only.

Card security details *must never be stored in any computer application system* at the University.

Note: When destroying the card security details, they should be crosscut shredded, incinerated, or pulped.

4.7 Card data received and processed online

Only the University's approved online payment facility can be used for payment by card online.

5. CARD DATA THAT CAN / CAN NOT BE STORED

5.1 Must never be known or written down

The following customer card data ***must never be known or written down*** by University personnel:

- Personal Identification number (PIN)
- Card stripe data

5.2 Must not be retained after processing

The following customer card data ***must not be retained*** by University personnel, and must be destroyed, immediately after processing the card transaction:

- Card verification code (CVC)
- Authorisation code

5.3 May be retained after processing

The following customer card data may be retained by the University under the Data Protection Act, but only if there is a defined business need to do so:

- Type of card (Visa/Mastercard/etc)
- All digits of the cards primary account number
- Expiry date
- Start date
- Name of Card holder

6. RESPONSIBILITIES & REPORTING CARD DATA IRREGULARITIES

6.1 Responsibility

The Head of Finance is responsible for ensuring that this policy is communicated to all applicable staff, adhered to and regularly reviewed, in particular the policies on:

- receiving card data
- transmitting card data
- processing card data
- storage of card data

6.2 Reporting non-compliance or irregularities

Any non-compliance with the policies in this document, or any other irregularities detected in respect of card and the use of cards, must be reported immediately to the Head of Finance.

6.3 Reporting to the Acquiring Bank

The University staff member receiving or processing the card details must report any irregularity concerning the failure of a card to process, or any other suspicious activities by the cardholder, to the Head of Finance who will inform the Acquiring bank (Lloyds via. Cardnet).

The police must also be informed if there is reason to believe a crime may have been attempted or committed

6.4 Employee awareness

Employees receiving or processing card data must have read and understood this Policy before handling such data.

6.5 Policy review

This policy should be regularly reviewed and kept up-to-date in line with changes to regulations.

Appendix 1. **Card Authorisation Form**

CARD AUTHORISATION FORM
(Payment by credit or debit card)

Customer details	
Name	
Address	
Telephone	

Nature of transaction	

Card details			
Card Type (circle)	*Mastercard / Visa (Credit card)* *Switch / Delta / Electron / Solo / Maestro / Visa debit*		
Card Number			
Valid from		*Expiry date*	
Issue No.(switch only)		*Please enter below the last 3 digits of your security number (which can be found on the back of your card on the signature strip).*	
Cardholders signature	*[Where a signature is not obtained because the transaction is taken over the phone, state 'Details taken by phone' in place of the signature.]*		

Office use only

Completed by		Date	

- - - - -- - -- Section below to be cross cut shredded after processing- - -- - - - -- - - --

Last 3 digits of security number	