NORWICH
UNIVERSITY
OF THE ARTS

Vice-Chancellor: Professor Simon Ofield-Kerr

DATA PROTECTION POLICY

Academic Registrar December 2022

Approved by Senate: December 2022

Next Review Date: December 2024

Contents

1. Policy Statement

This Data Protection policy sets out the University's obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018), the actions it will take to fulfil those obligations and the responsibilities of staff, students and third-party agents in relation to personal data. The policy applies to all individuals who may process personal data held on behalf of the University and will be of interest to all students, staff and other individuals about whom the University might hold personal data.

The main points of the policy are:

1. It is necessary to collect personal data from students, staff and other individuals in order for us to carry out our legal responsibilities, functions and manage our operations as an educational institution engaged in teaching, research and as an employer.
2. The University will adhere to the data protection principles as set out in the UK GDPR and the DPA 2018.
3. The University will record details about the personal and special category data that it processes in line with Article 30 of the UK GDPR and will keep this data up to date.
4. Students and staff must provide the personal data required by the University as part of the contract they enter into to either administer their education, or to facilitate their employment, and must keep this data up to date.
5. All staff, students and other individuals, where we hold their personal data, have the right to access details of their own personal and special category data processed by the University.
6. It is the responsibility of managers to ensure their staff are aware of the requirements of the data protection legislation when processing personal data.
7. Training on data protection is available to all staff from the induction process onwards.
8. Any deliberate or negligent breach of the requirements of the data protection legislation may result in disciplinary action being taken against the relevant member of staff or student.

2. The Principles of Data Protection Act 2018 and the UK General Data Protection Regulation

2.1 The principles to ensure that personal data is processed properly, and which the University follow to ensure it complies with the legislation, are set out on the Information Commissioner's Office website.

2.2 Under the UK GDPR and DPA 2018, personal data shall:

1. Be processed lawfully, fairly and in a transparent manner;
2. Be obtained for specified, explicit and legitimate purposes and not further processed in a manner that is at odds with those purposes (unless for archival, scientific or historical research purposes or statistical purposes);
3. Be adequate, relevant and limited to what is necessary;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept in an identifiable form for longer than is necessary for the purpose for which it was collected;
6. Be kept safe from unauthorised access, accidental loss, damage or destruction;

7. Not be transferred to a country outside of the EEA without appropriate safeguards being in place.

2.3 The University and its staff who process or use personal data must ensure that they follow these principles at all times.

3. Definitions

Many of the terms used in this policy are taken from the UK GDPR and DPA 2018 and are explained here:

Personal data: any information relating to an identified or identifiable living individual, including by reference to an identifier such as an ID number, location data or online identifier. Personal data includes special data as described below.

Special category data: personal data relating to issues of:

- the racial or ethnic origin of the data subject
- political opinions
- religious or philosophical beliefs trade union membership physical and / or mental health sex life or sexual orientation genetic data
- biometric data processed for the purposes of uniquely identifying a living individual criminal convictions or offences

Processing: the collective term for any action or set of actions relating to personal or special category data, including collecting, recording, organising, adapting, altering, storing, using, disclosing, erasure and destroying data. Processing also includes the transmitting or transferring of data to a third party.

Data Protection legislation: the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data subject: the individual who is identified by the personal data collected.

Data controller: the organisation that determines (alone or jointly with others) the need, purpose and means of processing personal data, and the uses to which it will be put. All departments, schools and sections of the University form part of the legal entity, which is the University, which is the data controller.

Data processor: a third party which processes personal or special category data on behalf of a controller.

Data Protection Impact Assessment: a risk assessment of any new processing, to protect the rights and freedoms of the data subject whilst allowing the data processing to continue.

Data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Third party: any external person or organisation that is neither the data subject nor the data controller.

Pseudonymisation: the processing of personal and special category data in a way that the data can no longer be attributed to a specific data subject without the use of additional information, which itself must be kept securely and separately from the pseudonymised data.

ICO: the Information Commissioner's Office, the supervisory authority for, amongst other things, the data protection legislation.

4. Registering with the ICO as a Data Controller

As an organisation that processes personal and specific category data, the University is required to pay a fee to the ICO which pays for the work of the ICO. The University provides the ICO with certain information to determine the level of the data protection fee payable. The ICO will publish contact details for the University and for the University's Data Protection Officer, fee information, any trading names used by the University and the data protection registration number given by the ICO (Z7289627)

5. Data Processed by Norwich University of the Arts

5.1 The University will maintain and use records of personal and special category data relating to staff, applicants, students, Alumni supporters and friends and business contacts of the University as is necessary and appropriate for its effective operation as an educational organisation, employer and conducting research.

5.2 Those whose personal information is held by the University will be notified at the point of data collection, by sending the appropriate Privacy Notice. This sets out what data is held, the legal basis, what it is used for, who it is shared with and how long it is retained. The Privacy Notices are available on the NUA website.

5.3 Where, in addition to this personal data, specific personal data is collected from students or staff for specific purposes, such as for educational trips or wellbeing purposes, this will be collected by consent. 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 be confirmed in writing with the data subject's signature particularly in the case of special category data. With the understanding that the consent can be withdrawn.

5.4 The University maintains a record of the data processing carried out across the University in accordance with Article 31 of the UK GDPR. This record contains the following information:

- Name and contact details of the University and of the University's Data Protection Officer, Sue White, dataprotection@nua.ac.uk
- Purposes of the processing and a description of the people from whom personal data is collected, and the types of data collected
- Details of third parties with whom the personal data might be / has to be shared

- Whether data will be transferred outside of the European Economic Area

5.5 The University must have a legal basis for its processing of personal data, as set out in Article 6 of the UK GDPR. Each of the legal basis may apply to the processing carried out by the University at any time, but those bases that the University will rely on most are:

- That the processing is necessary for the performance of a contract with the individual to whom the data relates
- That the processing is necessary for the compliance with a legal obligation on the University
- That the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the University
- That the processing is necessary for the purposes of the University's legitimate interests (although only in relation to certain of the University's activities)
- That the individual has given their consent to the processing

5.6 Students are formally asked to check the accuracy of their personal data annually at pre- enrolment and re-enrolment. Staff are formally asked to check the accuracy of their personal data at least once every two years. Students can update their data at any time by contacting registry@nua.ac.uk whilst staff are able to update their HR records at any time by contacting the HR Department.

5.7 It is necessary for the University to process special category data to operate or monitor University policies (e.g., sick pay, equality and diversity, to make the appropriate relevant adjustments for staff or students), to ensure the University is a safe place to work or study, or to enable the institution to comply with the law. Staff and students will be made aware of the sensitive nature of the information they are being asked for and will be asked to give separate explicit consent for the use of this data. The one exception to this would be if a situation occurred where there were concerns for the safety of the individual or another person. In such a situation, the UK GDPR allows special category data to be processed without referral to the individual in advance, where that person is incapable of giving their consent, as set out in Article 6(1)(d) of the UK GDPR.

5.8 Financial information is collected by the University's Finance department in order to pay staff, contractors and suppliers, and data is processed in accordance with the University's Financial Regulations. 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 (Appendix 10) sets out how the University controls the collection, transmission and storage of credit card data. All staff involved in credit card transactions are required to follow the policy and procedures laid down in Appendix 10 of this document.

6. Responsibilities of the University

6.1 The University as a corporate body is the 'Data Controller' under the data protection legislation, and the Board of Governors is therefore ultimately responsible for implementation of the data protection legislation, ensuring that the University complies with the legislation. The University could be fined for non-compliance with the UK GDPR. There are two tiers of fines depending on the type of infringement, detailed on the ICO website. Responsibility for the overall management of the implementation of the legislation lies with the Deputy Vice-Chancellor. Responsibility for implementing the provisions of this policy lies with the University's Data Protection Officer.

6.2 The University is a public authority as defined by the Freedom of Information Act 2000 and as such is required, under Article 37 of the UK GDPR, to have a Data Protection Officer. This work is carried out by our Compliance Manager.

6.3 The responsibilities of staff and students under this policy are outlined in sections 7 and 11 respectively below. Failure to follow the policy may result in disciplinary proceedings being brought by the University, whilst deliberate breaches of the data protection legislation may result in action being taken against the individual by the Information Commissioner's Office (ICO), the supervisory authority for this legislation.

6.4 Any individual who considers that the policy has not been followed in respect of their own personal data must raise the matter initially with the University's Compliance Manager. If the member of staff or student is unhappy with the steps taken by the University to resolve their issue, that individual retains the right to make a complaint to the ICO.

6.5 Any individual who believes that this policy has been contravened to the point that a data breach has occurred, should use the process outlined in the Information Security Incident Reporting Policy (Appendix 10 of this document) to notify the University.

7. Responsibilities of staff

7.1 All staff have the following responsibilities:

- To check, when requested, that any data they provide to the University in connection with their employment is accurate and up to date
- To inform the University of any changes to, or errors in, the data held
- To comply with the guidelines for staff in section 7.2 below if, and when as part of their responsibilities, they process data about other people.

7.2 Staff whose work involves the use of personal data are responsible for ensuring that:

- When collecting personal or special category data, they collect only the minimum amount of data necessary to complete the work for which the processing is necessary
- They provide sufficient information to explain the reasons f or the data processing by providing them with the relevant Privacy Notice (see section 5)

- They carry out a Privacy Impact Assessment (PIA) whenever necessary (see section 15 for more information on PIAs)
- They anonymise personal data as soon as possible and wherever appropriate
- When employing a third party as a processor, that third party is made aware of their responsibilities under the UK GDPR
- Any personal data that is held in hard copy or electronically is kept securely, in locked cabinets or through the use of password protection, encryption of electronic files where necessary, access controls and anonymisation
- Personal data is not disclosed by them orally or in writing, to any unauthorised third party
- The personal data is accurate and kept up to date where appropriate, held for the appropriate length of time and destroyed confidentially when / if it is no longer needed, in line with the University retention schedule
- They do not access any personal data which is not necessary for their work.

7.3 Staff who are processing personal data for project or research purposes must obtain the approval of the NUA Research Ethics Committee.

7.4 Managers have an additional responsibility to ensure that their staff are aware of the data protection legislation principles and know how to correctly process personal and special category data as part of their work. Managers should also ensure that their staff have taken the mandatory Information Security Awareness training and the Data Protection Awareness training. Information will be provided by the HR Department.

7.5 All staff should be aware of and adhere to the IT Acceptable Use Policy and the Information Security Policy in addition to this Data Protection policy

7.6 Any deliberate or negligent breach of these responsibilities – or of the statutory obligations of the DPA 2018 and UK GDPR – may result in disciplinary action being taken against the relevant member of staff.

8. Responsibilities of students

8.1 Students must assist the University in ensuring that all their own personal data as provided to the University at registration is accurate and up to date. Students who need to notify the University of any subsequent changes in their personal details can do so by contacting registry@nua.ac.uk

8.2 Students may themselves need to process personal data for project or research purposes (for example, in carrying out surveys) or they may be employed by the University in a part- time job that handles staff or student personal data. If students are carrying out projects or research work, they must notify their tutor and obtain the approval of the Learning, Teaching and Quality Committee Ethics Committee (Undergraduate and Postgraduate Taught students) and the NUA Research Ethics

Committee (Postgraduate Research Students) as to the need to process the data before collecting any personal data.

8.3 Students employed by the University in positions that allow access to personal data about any student, applicant or member of staff must abide by the responsibilities for staff as set out in paragraph 7.2 above and take care not to access any personal data about anyone not related to the work being carried out.

8.4 It is good practice, where a student is employed as a member of staff, for the student's access to personal data to be restricted only to areas of the University in which they do not work or study or know any students.

9. Data Processor responsibilities

9.1 Under the UK GDPR, there are responsibilities for data processors, that is, a third party that carries out data processing actions on behalf of, and on the instructions of, a data controller. The responsibilities (section 9.2 below) must be pointed out to the data processor at the beginning of the contract between both parties.

9.2 If a data processor is employed to carry out work on behalf of the University, staff must ensure that the contract sets out the University's own responsibilities in relation to the data processing (the instructions for processing and security requirements of the data processor) and contains the following information in relation to the data processor's responsibilities:

1. the data processor can only process data in the ways set out in the contract
2. the data processor's staff must be trained in secure data processing methods and understand the confidentiality aspects of their work
3. appropriate security measures are taken for the personal data being processed
4. the processor can only engage a sub-processor with the agreement of the University and on the terms required by the University
5. the processor provides assistance to the University in dealing with data subject rights, where requested by the University, and
6. the data processor either deletes or returns the personal data to the University at the end of the contract.

10. Disclosure

10.1 Under Data Protection legislation, the University must not disclose data to unauthorised third parties. A 'third party' includes family members, friends and external agencies.

10.2 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 e.g., 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 (e.g., informing the student's LEA or sponsor of course changes/withdrawal).

10.3 The University's Privacy Notices provide more detailed information about who we may share data with. 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.

10.4 With the exception of (iii) it is necessary that the University's Compliance Manager be informed in order that appropriate procedures are followed.

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

(i) References for current or prospective employers or educational institutions.

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

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

10.6 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 Section 17 References.

10.7 Students are given the opportunity to opt out of 10.5 (iii) when they apply for Graduation tickets, and they may notify the Academic Registrar in writing at any time up to 10 days before Graduation.

11. Disclosure to the Police

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

11.2 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 Compliance Manager and should be writing, unless it is felt that it is a life and death situation.

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

12. Disclosure of information about students in receipt of learning support

12.1 Explicit consent must be given by students to release this information as this is special category data. 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.

13. Disclosing personal data overseas

13.1 The UK GDPR requires any personal data which is transferred out of the UK to be adequately protected. The UK Government has deemed some other countries (the EEA, as detailed in 13.3 below) to have adequate data protection regimes, so data may be transferred to these countries more freely. The EU has made a similar adequacy decision for the UK which means that we can transfer personal data in and out of the EU without the need for additional agreements.

13.2 As detailed above, Data Protection legislation contains specific provisions with regard to the transfer or personal data outside of the EEA. 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.

13.3 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 and Sweden and the EEA also includes Norway, Iceland and Liechtenstein.

13.4 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.

13.5 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. Data Subject Rights

14.1 Data Protection 'Rights of the Data Subject'
Staff, students and other individuals where the University holds their personal information have rights under the UK GDPR in relation to the processing of their personal data. Sections 14.2 to 14.8 detail those rights. For more information on how to exercise these rights please contact the University Compliance Manager, Sue White at dataprotection@nua.ac.uk

14.2 Subject Access Rights
Individuals have the right to be informed about how their personal data may be processed (see information on Privacy Notices at section 5). In additional they have the right to access any personal data that is being kept about them by the University. Further information on the Subject Access Request process, what information will be accessible and how to receive copies of their personal data is available in Appendix 2. The University will comply with requests for access to personal data within one month of receipt of the request.

14.3 Right to rectification
If an individual believes that the University holds inaccurate personal data about them, they have the right to have the data rectified.

14.4 Right to erasure (to be forgotten)
Individuals have the right to have personal data relating to them erased from the University's systems in certain circumstances, although the UK GDPR allows for situations where the right of erasure may not be applicable (Article 17(3)), so this is not an absolute right.
Personal data must be erased on request

- Where it is no longer necessary for the personal data to be held
- Where the consent given for the processing is withdrawn (and no other legal basis exists for retaining the data)
- Where the individual objects to the processing for public and legitimate interest reasons (unless the University can prove compelling legitimate interests to continue the processing)
- Where the personal data was processed unlawfully in the first place

- Where the personal data must be erased in compliance with a legal obligation, and
- Where the personal data was collected in relation to marketing

14.5 Right to restrict processing

Individuals can require the University to restrict processing of their personal data, that is, temporarily stop or no longer allow any future processing of their personal data, in situations where:

- The accuracy of the personal data is in question
- The processing is unlawful, but the individual does not want the data erased
- The University no longer needs the personal data, but the individual requires its retention for legal reasons, or
- The individual has objected to processing based on the legal basis of public or legitimate interests.

14.6 Right to data portability

Where an individual has given their consent to their personal data being processed by the University, and the processing is carried out automatically, the individual has the right to either receive a copy of that data in a machine-readable format or to have that data transmitted directly to another data controller.

14.7 Right to object

An individual can object to the processing of their personal data in the following circumstances:

- When the processing is based on the legal basis of either being in the public interest or the legitimate interests of the University
- Where the processing is for direct marketing purposes
- Where the processing is for scientific or historical research purposes, or statistical purposes

– unless the processing is necessary for the performance of a task carried out for reasons of public interest.

14.8 Right not to be subject to automated decision-making

Individuals have the right not to have decisions made about them solely through automated processing where that decision will have a legal effect.

14.9 You are entitled to take your case to court to: enforce your rights under data protection law if you believe they have been breached: claim compensation for any damage caused by any organisation if they have broken data protection law, including any distress you may have suffered.

15. Data Protection Impact Assessments

15.1 The UK GDPR requires data controllers to complete an assessment of potential risks to the rights and freedoms of individuals when new technologies are used for data processing, where large amounts of special category data are processed or where automated decisions (including profiling) will take place that will lead to decisions that can have a legal effect on the individual.

15.2 A Data Protection Impact Assessment (DPIA) should be started as early as possible in a project and revisited at key stages in the project - at review points or milestones - or as and when changes to the project take place. This is necessary to ensure that the data protection principles and the rights of data subject remain central requirements in all applicable projects. The outcomes of this process will include appropriate consideration of privacy by design, the level of security needed for the personal data being processed, and the proper management of the data when it is no longer needed, either through anonymization or destruction.

15.3 The Compliance Manager can provide the relevant assessment paperwork and provide advice and guidance.

16. Use of Personal Data in Academic Research

16.1 Research

16.1.1 Whilst one of the principles of the UK GDPR is that personal data shall not be processed for any reason other than the purpose for which it was collected (Article 5.1.b.), further processing for research or statistical purposes is allowed under Article 89(1), so long as safeguards for the rights and freedoms of the individual concerned are implemented.

16.1.2 These safeguards include the idea of data minimisation, pseudonymisation or anonymisation of the data to reduce the possibility of identification of the individual.

16.1.3 Once personal data has been anonymised to the point where a living individual can no longer be identified by it, the data ceases to be personal data and therefore the constraints of the UK GDPR no longer apply.

16.1.4 The personal data cannot be processed in a way that it will have a direct effect or result on the identifiable individual, or in such a way as to cause damage or distress to the individual.

16.1.5 The legal basis for processing personal data in most research projects will be that the individual has given their consent to the processing.

16.1.6 It is important when recruiting participants for research projects, to reassure them that their data will be processed in accordance with the UK GDPR and that they have the right to see the data that is held about them, unless it has been anonymised so that they can no longer be identified.

16.1.7 All research involving use of personal data must be carried out according to the principles set out in the NUA's Code of Practice on Research Ethics (staff and postgraduate research students) or the Code of Ethics for Undergraduate and Taught Postgraduate Students (all other students) as well as this policy. Approval for any research involving personal data must be obtained through the relevant ethics approval procedure.

16.2 Research and external organisations

16.2.1 Personal data should only be provided to third parties if this has previously been agreed by the data subjects. There must be a written agreement in place to govern the deployment, ethical use, integrity and security of the data. This written agreement must also stipulate the third party's obligations to retain the data for a defined period of time, and to destroy the data when it is no longer needed. There must also be procedures in place to ensure that the transfer of all personal data is secure.

16.2.2 If you are using personal data that has been provided by another organisation then you must ensure that your research is compatible with what the data subjects were told would happen to the data, unless the personal data is anonymised to the point where the individuals cannot be identified by the data.

16.2.3 Activities that involve third parties who are contracted to secure or collect data on behalf of the University must be carried out according to the principles set out in the relevant ethics code (see 16.1.7) as well as this policy.

17. References

17.1 Personal references are exempt from subject access requests.

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

17.3 It is the University's policy that staff references are provided by HR Department. Staff who are contacted by a member of staff to provide a reference should contact HR and take advice.

17.4 Student references can be provided on request by the student. Guidance is published on the University's intranet Writing Student References: A Guide for Academic Staff. Where a member of academic staff is unable to provide a reference, Academic Registry can provide a letter confirming the student's course, period of registration and award (where applicable).

17.5 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.

17.6 Before providing the reference, it is necessary to ensure that:

- the information is factually correct;
- the minimum amount of data is disclosed;
- Special category 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, only those that could be justified should be provided.

17.7 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.

17.8 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.

17.9 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.

18. Retention and disposal of data

18.1 The University is committed to keeping and disclosing personal data in a responsible and secure manner and will therefore keep data for the minimum time necessary to fulfil its purpose. The University will maintain a comprehensive Retention of Records schedule to help avoid excessive retention or premature destruction of personal data.

18.2 The University will keep enough data about a student to be able to confirm the qualifications achieved whilst at the University. Any other data will be removed from student files six years after the student graduates or otherwise leaves the University.

18.3 The University will keep basic employment history data about former employees for 100 years from the staff member's date of birth in order to verify employment details. Most other data will be removed a minimum of six years after their employment with the University has finished, in order to meet data needs for pensions, taxation, potential or current disputes or job references. The University will also keep the health and safety records of accidents that happen to visitors to the University for three years after the date of an accident.

18.3 Personal data that is no longer required will be destroyed in as secure a manner as possible. Paper based records will, at least, be put in a confidential waste sack or confidential waste bin for collection as soon as possible by the Estates Team. Records containing special category data should be shredded. Electronic records will be deleted if hardware such as hard drives, laptops, smart phones, photocopier / printers etc. are decommissioned. The ITS department will dispose of data and hardware in accordance with the Procedures for the Secure Disposal of IT Hardware (Appendix 5 of the University's Information Security Policy).

18.4 Any processing or storing of University information on personally owned devices must be in compliance with NUA's policy on Mobile and Remote working (Appendix 8 on the Information Security Policy). This includes the secure disposal of data.

19. Related information

This policy should be read in conjunction with the following information,

- ICT Acceptable Use policy
- Information Security policy
- Privacy Notices
- Freedom of Information webpages

Appendix 1

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 (e.g., 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 (egg. 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 (egg. course evaluation document), care should be taken to avoid identifying people by name without their permission.

Photography and filming

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

Photographs or films 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 (egg. 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 13 Disclosing personal data overseas for further guidance about the transfer of data used in the University's publicity.

Appendix 2

Appendix 2: Subject Access Requests

Data Protection legislation 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" (SAR).

Although it is not a legal requirement for SARs to be made in writing, individuals are encouraged to complete a SAR form, available on the University's website, so we can ensure we have a full understanding of what data is being requested. In order to ascertain what data is required, the data subject will be expected to provide information to assist the University in its ability to locate the specific information required.

It should be noted that, to ensure there is no unauthorised disclosure of personal information, no data will be released until documentation is provided which verifies the data subject's identity.

The response should detail:

- information on whether personal data is held by the University
- a description of the data and a record of the purposes for which it is being processed
- a copy of the data, together with an explanation of any codes/jargon, if needed.

The University must respond to Subject Access Requests within one month. In complex cases where the gathering of information is likely to take longer than this period or where the Compliance Manager requires more specific information on the data required from the data subject, the individual will be informed in writing, subject to a maximum time of two further months.

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 p arty 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 Compliance Manager when they wish to make a Subject Access Request.

Appendix 3

Appendix 3: Disclosure of Student Information and Use of Data

This appendix provides additional guidance to sections 10 to 13 of this policy.

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 it 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 is available from the Student Enquiries Office, Academic Registry or Student Support.

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 (Course Administration). 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 file 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 makes every effort 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

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. Summative feedback is made using the Online Assessment Feedback System and once published is available to students.

Where any other comments are made on an assessment script and where the script is not made available by 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/PG Cert Boards and 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 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, any references to other individuals are anonymised.

The University can only consider refusing to provide this information 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. All assessment results, including final awards, are published to individual students online via the e:Vision portal.

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 (egg. 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 (egg. 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

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 at 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 (egg. 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 special category 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 (egg. 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 if 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, for example 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

Appendix 6: Records Management

The University recognises 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 'Records Management Guide'.

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 (ISO 15489: 2001).

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 Act 2000 and DPA 2018 and UK GDPR) 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

Appendix 7: Student Records Management

Procedures for staff regarding the storage and processing of student records.

For the University to function efficiently a formal student record (in paper form) is held in the course area, 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 and in secure folders on the University's IT servers. All student data held 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.

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 special category 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 letters 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). Special category 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 (egg. formative feedback notes 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 (egg. tutor's notes), the same precautions in respect of storage and security apply. Reference should be made to the Data Protection policy regarding security.

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 (egg. 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 special category 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 ap peals and complaints will be kept for a period of eight years.

Appendix 8

Appendix 8: Student Consent to Release Information Pro Forma

Student Consent to Release Information (General)

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 _____

I understand that I can withdraw my consent at any time by contacting registry@nua.ac.uk

Signed _____ Dated _____

For Office Use

Consent recorded on register	Consent filed

Student Consent to Release Information (Student Support)

Student Consent for Third Parties

SECTION A: DETAILS		
Surname/Family Name	**First and other names (in full)**	
Course title (in full)	**Date of birth**	**Student number (as on ID card)**
I authorise staff from Norwich University of the Arts to discuss information relating to my studies, finances and/or welfare with:		
Name and Relationship to you/ Type of Organisation	**Address and contact details**	
Name and Relationship to you/ Type of Organisation	**Address and contact details**	
Name and Relationship to you/ Type of Organisation	**Address and contact details**	

SECTION B: DECLARATION
I consent to the release of the information I have provided on this form and in accordance with Norwich University of the Arts notification under the Data Protection Act 2018. Signed: Date:

When completed, please send this form to: support@nua.ac.uk from your Norwich University of the Arts email address

This document will be active from the date on which the form has been signed.

Office Use

Date Received		**SS Initial**	

Appendix 9

Appendix 9: 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 and
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 salesperson has a card terminal, it is essential that customers enter their PIN (Personal Identification Number) into the card terminal unobserved. This includes ensuring that CCTV cameras are not positioned in such a way that they could inadvertently pick up a customer entering his/her PIN. 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 should 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. They must be stored for at least 13 months (in order to comply with banking Chargeback regulations) but soon after this time period has elapsed, the details should be destroyed.

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.

4.8 Awareness of suspicious behaviour

Those responsible for card terminals should ensure that they verify the identity of third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices.

Staff should also be aware of suspicious behaviour around devices (for example, attempts by unknown persons to unplug or open devices). Any such behaviour or indications of device tampering, or substitution should be reported to the Director of Finance without delay.

5. Card data that can / cannot 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

These details must be stored for at least 13 months (in order to comply with banking Chargeback regulations) but soon after this time period has elapsed, the details should be destroyed.

6. Responsibilities & reporting card data irregularities

6.1 Responsibility

The Director 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 Director 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 Director of Finance who will inform the acquiring bank.

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.

Card Authorisation Form

NORWICH UNIVERSITY OF THE ARTS

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 crosscut shredded after processing - - -- - - - -- - - --

Last 3 digits of security number	

Appendix 10

Appendix 10: Information Security Incident Reporting Procedures

1. Introduction

This document outlines the procedures for reporting information security incidents.
Information security incidents or breaches can be caused through human error or malicious intent and are on the increase. With the changes in technology and the growth in information creation, processing and storage, the challenge of keeping information safe increases also.
It is essential that NUA has in place a robust and systematic process for responding to an information security incident to protect its information assets.
By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated
- incidents are handled by appropriately authorised staff
- appropriate levels of University management are involved in response management
- incidents are recorded and documented
- the impacts of the incidents are understood and action is taken to prevent further damage
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny
- external bodies or data subjects are informed as required
- the incidents are dealt with in a timely manner and normal operations restored
- the incidents are reviewed to identify improvements in policies and procedures.

2. Definition

A security incident or breach is any real or suspected unauthorised access to, or loss of NUA data. These include:

- Equipment failure, including through f ire or flood.
- Loss or theft of data or equipment upon which data is stored
- Unauthorised access to confidential information
- Social engineering attack
- Human error
- Cyber or hacking attack

3. Scope

This information security policy appendix is applicable to all NUA employees, students, contractors, visitors and data processors acting on behalf of the University.
Any data or information that is rated as “confidential” according to the University’s Information Classification scheme (Appendix 4 – Information Classification and Handling policy) is subject to these incident reporting procedures in all formats (digital, paper etc.).

4. Responsibilities

Information users: Anyone who has access to information has a duty to report any suspected, real, threatened or potential information security incidents. They will provide further assistance with any ongoing investigations as required

Line Managers: Line managers ensure that their teams within their areas of responsibilities act within accordance with this policy and will assist with investigations as required.
Senior Management: Will oversee the management of the information security incident delegating as necessary.
In the first instance any suspect incident or breach should be reported to the Compliance Manager.

5. Information Security Incident Reporting

Suspected or confirmed information security incidents or breaches should be reported immediately. The form should be emailed to servicedesk@nua.ac.uk and the Compliance Manager at dataprotection@nua.ac.uk and also contact 6499 (or 01603 751499) to advise Service Desk staff that an Information Security Incident Reporting form has been sent.

The report should include:

- Full and accurate account of the incident
- Name(s) of the person(s) involved
- Nature of the information involved

The Incident Reporting form should be used to provide details: see appendix. After the reporting of an incident, an assessment will be carried out to determine the extent and severity of the incident.

The Compliance Manager will log the incident and provide oversight for the investigation. Where the Compliance Manager and IT Manager are in agreement that the resultant risk to any individual's rights and freedoms is minimal to low, the Compliance Manager will respond to the parties in writing, identifying any further training necessary and justifying their reasoning for the decision that no further action is necessary. This email will be retained within in the incident log.

The UK General Data Protection Regulation (UK GDPR) makes it clear that when a security incident takes place, you should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the Information Commissioners Office (ICO) if required. Any reportable breach must be reported to the ICO within 72 hours of the incident being discovered.

6. Information Security Management Plan

The following plan will be used in the investigation of any incident:

i. Containment and recovery
ii. Risk assessment
iii. Requirements for further notifications
iv. Evaluation and response

A detailed breakdown of these four points can be found in Appendix 2.

When a personal data breach has occurred, we will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk, then we will notify the ICO. If we decide we do not need to report the breach, we will justify this decision, and document it.

Information Security Incident Reporting

1. Information Security Incident Reporting Form

Incident Number: (For IT/DR Use)		**KACE Ticket No:** (For IT/DR Use)	
Description of the Information Security Incident:			
Date / Time of incident or when incident was identified:			
Person reporting incident: Name, role, department			
Nature of the information involved: Type; amount; format etc.			
Confirmed incident or suspected?			
Is incident continuing or is it contained?			
What actions have been taken so far to stop incident or recover information?			
Who has been informed so far?			
Other relevant information? Computer ID number, email addresses, others involved etc.			
Email form to servicedesk@nua.ac.uk & Compliance Manager at dataprotection@nua.ac.uk and contact 6499 (or 01603 751499) and advise Service Desk staff that Information Security Incident Reporting form has been sent.			
Received by:			
Date / Time:			

2. Containment and Recovery Check Lists – For Compliance Manager/ITS use

To limit the spread of any incident and its consequences and to endeavour to recover any lost information.

Step	Action	Notes
1	Compliance Manager/IT Services Manager (or designated authority) to determine the severity and spread of an incident and what data or information is involved	
2	Compliance Manager and/or ITSM to lead investigation into incident bringing in additional expertise as necessary (ITS / Registry etc.)	
3	Investigate the cause of the incident, what information was affected and the extent. Act to stop further breaches or data loss.	
4	Commence recovery of lost data and further limit any damage. Recovery from backups, re-installation of systems etc.	
5	Reporting to the police and other organisations as necessary	
6	Logging and recording of all key actions and decisions for later analysis	

3. Risk Assessment Check List:

To determine the risks associated with the security incident and the impact.

Step	Action	Notes
7	The amount and type of information involved and classification	
8	Description of the data/information involved. Academic records, bank details etc.	
9	Information lost, stolen or corrupted?	
10	If information was lost or stolen was data or device encrypted?	
11	If information was damaged or corrupted are there mitigations in place? e.g., Backups, copies etc.	
12	How many people are affected by the incident and who are they? Staff, students, applicants, suppliers etc.	
13	What is the nature of the information that has been stolen / lost? Consideration of what data might be used for.	
14	What is the potential for harm / distress to individuals whose information has been compromised?	
15	What are the wider consequences of the incident? Reputational damage, legal implications, financial loss?	
16	Other sources of advice and expertise. E.g., contacting banks if financial details are lost	

4. Requirements for further notifications:

Who else needs to be notified? Is it necessary to inform the ICO?

Step	Action	Notes
17	Who else should be notified? Contractual, legal or regulatory, e.g., funding body, collaborative partner etc.	
18	Would notification prevent further loss, unauthorised access or damage?	
19	Would notification help individuals involved? e.g., as a prompt to change passwords, monitoring bank accounts etc.	
20	Consider whom to notify, what the message is and how this will be communicated to those affected. VC/DVC, AcR and Director of Marketing if external.	

5. Evaluation and response

Step	Action	Notes
21	Review situation and determine if there are further risks that need to be mitigated. What is required to prevent a repeat?	
22	Review the data, how it is stored and where and for how long? Are there any changes required in light of the incident?	
23	Carry out complete review of the existing security measures and procedures in light of the breach. What improvements need to be made?	
24	Carry out gap analysis of all training and awareness. Improve training and advice.	
25	Provide a report to senior team. With recommendations, costings etc.	

6. Incident Management Timeline

Date	Time	Activity	Decision	By Whom?

Strategy & Policy Revision Sheet

1.	**Name of Document:**	**Data Protection Policy**
2.	**Originator:**	**Academic Registrar**
3.	**Date of Origination: Version 1**	Date not recorded
4.	**Senate* Ratification:**	N/A
5.	**Assigned Ref Number:**	SDP015
6.	**Revision History** **Revision 1** **Senate* Ratification:** **Assigned Ref Number:**	 5 September 2008 University updates N/A SDP015
	Revision 2 (b) **Senate* Ratification:** **Assigned Ref Number:**	1 January 2009 New Principal updates SD/P/015b
	Revision 3 (c) **Senate* Ratification:** **Assigned Ref Number:**	30 January 2013 Inclusion of the Credit Card Security Policy in section 5.3 and Appendix 10. Amendment to Appendix 8: retention of appeals and complaints records changed to 8 years. 30 January 2013 SD/P/015c-U1
	Revision 4 **Senate* Ratification:** **Assigned Ref Number:**	25 May 2018 Major revision in accordance with General Data Protection Regulations and Data Protection Act 2018 6 June 2018 SD/P/015-U2
	Revision 5 **Senate* Ratification:** **Assigned Ref Number:**	6 June 2020 Minor error correction N/A – owner approval SD/P/015-U2

	Revision 6 **Senate* Ratification:** **Assigned Ref Number:**	6 October 2022 Revisions in accordance with UK GDPR and updates in relation to SAR processes 1 December 2022 SD/P/015-U2
7.	**Destruction Date Confirmation:**	N/A