DATA PROTECTION POLICY

Originator: Prof. Dave Russell
Date: January 2012
Approved by: SMT
Type: Policy

Revised: 18/5/18
Updated: 30/4/19

CONTENTS

1. Introduction 3

2. Status of the policy 3

3. Notification of data held and processed 3

4. Responsibilities of staff 4

5. Data security 4

6. Student obligations 5

7. Data subjects rights 5

8. Subject consent 6

9. Privacy by design and data protection impact assessments 6

10. The Data Controller and the designated Data Controllers 7

11. Reporting a personal data breach 7

12. Transfer limitation 8

13. Retention of data 8

14. Summary 8

APPENDIX A: Glossary 10

1. INTRODUCTION

1.1 Leeds Arts University ("the University", "we" or "our") obtains, uses, stores and otherwise processes Personal Data relating to potential staff and students (applicants), current staff and students, former staff and students, current and former workers, contractors, website users and contacts (Data Subjects). When Processing their Personal Data, the University is obliged to fulfil individuals' reasonable expectations of privacy by complying with the General Data Protection Regulation 2018 (the GDPR) and the Data Protection Act 2018 (DPA).

1.1.1 To do this, we must comply with the Data Protection Principles which are set out in the GDPR. In summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and in a transparent manner
- Be obtained only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
- Be accurate and where necessary kept up to date.
- Not be kept in a form that permits identification of Data Subjects for longer than is necessary for that purpose.
- Be processed in a manner that ensures its security, using appropriate protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

1.2 All staff or others who process any personal data must ensure that they follow these principles at all times. In order to ensure that this happens, the University has developed the Data Protection Policy.

2. STATUS OF THE POLICY

2.1 It is a condition of employment that employees will abide by the rules and policies made by the University. Any failures to follow the policy can therefore result in disciplinary proceedings.

3. NOTIFICATION OF DATA HELD AND PROCESSED

3.1 Whenever we collect Personal Data directly from Data Subjects, for example for the recruitment and employment of staff and for the recruitment and enrolment of students, at the time of collection we will provide the Data Subject with the following information:

- University's details;
- Contact details of our DPO;
- Purposes of processing;
- Legal basis of processing;
- Where the legal basis is legitimate interest, identify the particular interests (e.g. marketing, fundraising);
- Where the legal basis is consent, the right to withdraw;
- Where statutory/contractual necessity, the consequences for the Data Subject of not providing the data of non-provision.

When Personal Data is collected indirectly (for example, from a third party such as UCAS or publically available source), we will also check that the Personal Data was collected by the

third party in accordance with the GDPR and on a basis which considers our proposed processing of that Personal Data.

3.2 To satisfy the above, the University will provide all staff and students and other relevant users with a Privacy Notice. This will state all the types of data we hold and process about them, where it was sourced from and the reasons for which it is processed.

4. RESPONSIBILITIES OF STAFF

This policy applies to all Personal Data we process regardless of the medium on which that Personal Data is stored and regardless of who the Data Subject is. Pro-Vice-Chancellors, Programme Directors, Course Leaders, heads of support areas and workshop managers are responsible for ensuring that staff within their area of responsibility comply with this policy. All staff have a responsibility to comply with Data protection law and we will provide training to enable this, which must be undertaken.

The Data Protection Officer (DPO) is responsible for overseeing this policy and for developing related policies and privacy guidelines. The University's DPO is Katie Machin, ext. 8280, dpo@leeds-art.ac.uk.

4.1 All staff are responsible for

- Checking that any information that they provide to the University in connection with their employment is accurate and up to date.
- Informing the University of any changes to information which they have provided. i.e. changes of address.
- Informing the University of any errors or changes. The University cannot be held responsible for any errors unless the staff member has informed the University of them.

4.2 Staff should only process Personal Data when performing their duties requires it and should not process Personal Data for any reason unrelated to their job duties.

4.4 Designated staff are responsible for ensuring that when Personal Data is no longer needed it is deleted or anonymised in accordance with the University's Records Retention Schedule.

5. DATA SECURITY

5.1 Staff must comply with all applicable aspects of our Staff Computer Use Security Policy and are responsible for ensuring that:

- Any personal data which they hold is kept securely.
- Personal data is not disclosed either verbally or in writing whether that is accidental or otherwise, to any unauthorised third party.

5.2 Staff should note that unauthorised disclosure and/or failure to adhere to the requirements set out in 5.3 to 5.7 inclusive below will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

5.3 Personal data should be;

- kept in a locked filing cabinet; or

- in a locked drawer; or
- if it is computerised, be password protected; or
- password protected if kept on portable media.

5.4 Personal data should never be stored at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites.

5.5 Ordinarily, personal data should not be processed at staff members' homes, whether in manual or electronic form, on laptop computers or other personal portable devices or at other remote sites. In cases where such off-site processing is felt to be necessary or appropriate, the agreement of the relevant Data Controller must be obtained, and all the security guidelines given in this document must be followed.

5.6 Data stored on portable electronic devices or removable media is the responsibility of the individual member of staff who operates the equipment. It is the responsibility of this individual to ensure that:

- Suitable backups of the data exist.
- Sensitive data is appropriately encrypted.
- Sensitive data is not copied onto portable storage devices without first consulting a Data Controller, in regard to appropriate encryption and protection measures.
- Electronic devices such as laptops, mobile devices and computer media (USB devices, CD's etc.) that contain sensitive data are not left unattended when offsite.

5.7 For some personal data, the risks of failure to provide adequate security may be so high that it should never be taken home. This might include payroll information, addresses of students and staff, disciplinary or appraisal records or bank account details. Exceptions to this may only be with the explicit agreement of a Data Controller (see 12).

6. STUDENT OBLIGATIONS

6.1 Students should ensure that all personal data provided to the University is accurate and up to date. They should ensure that changes of address, etc. are notified to the Course Administrator.

7. DATA SUBJECTS' RIGHTS

7.1 Data Subjects have rights in relation to the way their Personal Data is handled. These include the following:

- where the legal basis of our Processing is Consent, to withdraw that Consent at any time;
- to ask for access to their Personal Data that we hold;
- to prevent our use of their Personal Data for direct marketing purposes;
- to ask us to erase Personal Data without delay if:
  - it is no longer necessary in relation to the purposes for which it was collected;
  - the only legal basis of Processing is Consent and that Consent has been withdrawn and there is no other legal basis on which we can Process that Personal Data;
  - the Data Subject objects to our Processing where the legal basis is the pursuit of a legitimate interest or the public interest and we cannot demonstrate this;
  - the Data Subject has objected to our Processing for direct marketing purposes;
  - the Processing is unlawful.

7.2 In addition, they are entitled to receive further information about the processing of their Personal Data as follows:

- the purposes;
- the categories of Personal Data being processed;
- recipients/categories of recipient;
- retention periods;
- information about their rights;
- the right to complain to the ICO;
- details of the relevant safeguards where Personal Data is transferred outside the European Economic Area (EEA);
- any third-party source of the Personal Data.

7.3 In order to gain access, an individual may wish to receive notification of the information currently being held. We aim to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within one month unless there is good reason for delay. In such cases, the reason for delay will be explained in writing to the data subject making the request.

Where a Data Subject has required their Personal Data to be rectified or erased, we will inform recipients of that Personal Data that it has been erased/rectified within one month, unless it is impossible or significantly onerous to do so.

8. SUBJECT CONSENT

8.1 In most cases data processing is necessary for the performance of a contract with the Data Subject. This is the main basis under which we process personal data, either as a condition for staff as part of employment or for students to undertake a course.

8.2 Sometimes it is necessary to process sensitive personal data such as data revealing a person's health, criminal convictions, race and gender and family details. This may be to ensure the University is a safe place for everyone, or to operate other policies, such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern to individuals, Data subjects will be asked to give specific consent for the University to do this. Offers of employment or course places may be withdrawn if an individual refuses to consent to this, without good reason. More information about this is available from the DPO.

8.3 Consent needs to be renewed if we intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

8.4 In order that we can demonstrate compliance in this respect a record of all consents for enrolled students is maintained by the Academic Registry, a record of all consents for prospective students, alumni and those who have shown an interest in events at the University is maintained by Marketing, a record of consents made by staff is held by HR.

9. PRIVACY BY DESIGN AND DEFAULT AND DATA PROTECTION IMPACT ASSESSMENTS (DPIAs)

We will implement Privacy-by-Design measures when processing Personal Data, by using appropriate technical and organisational measures (like pseudonymisation) to ensure compliance

with data-protection principles. We will ensure only Personal Data which is necessary for each specific purpose is processed. We will carefully consider the amount of Personal Data we collect, the extent of its processing, the period of its storage and its accessibility. In particular we will control the number of people to whom it is available. Staff should ensure that they adhere to those measures within the Staff Computer Use and Security Policy. For example in the use of special access controlled drives for sharing access to personal data and encryption in the event that the use of attachments cannot be avoided.

We will also conduct DPIAs in respect of high-risk Processing before that Processing is undertaken.

We will conduct DPIA's in the following circumstances:

- the use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- automated Processing including profiling and Automatic Decision Making (ADM);
- large scale Processing of Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area. (eg CCTV)

A DPIA will include:

- a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk-mitigation measures in place and demonstration of compliance.

10. THE DATA CONTROLLER AND THE DESIGNATED DATA CONTROLLERS

10.1 The University is the data controller under the legislation however, there are designated data controllers who deal with day to day matters.

We have 3 designated 3 data controller:

Sharon Bailey	-	Pro-Vice-Chancellor Assurance and Director of Finance
Graham Curling	-	Head of Human Resources
Prof. Dave Russell	-	Pro-Vice-Chancellor Student Experience and Resources

The Data Protection Officer (DPO) is responsible for overseeing this policy and for developing related policies and privacy guidelines. The University's DPO is Katie Machin, ext. 8280, dpo@leeds-art.ac.uk.

11. REPORTING A PERSONAL DATA BREACH

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator including the Information Commissioners Office (ICO) where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, you should immediately contact the Universities Data Protection Officer and the appropriate SMT member according to the

procedures described in our Data Breach Management Guidelines.

Records of Personal Data Breaches must be kept, setting out:

- the facts surrounding the breach
- its effects; and
- the remedial action taken

These records will be maintained by the DPO and in accordance with the University's Data Breach Management Guidelines

12. TRANSFER LIMITATION

We may only transfer Personal Data outside the EEA if one of the following conditions applies:

- the European Commission recognises that the area or territory concerned has an adequate level of protection for the Data Subjects' rights and freedoms.
- we have in place our own safeguards such as a standard transfer agreement.
- the Data Subject has provided consent to the proposed transfer after being informed of any potential risks; or
- it is for the performance of a contract between the University and the Data Subject (e.g. a student's period abroad in an overseas institution/placement),
- reasons of public interest,
- to establish, exercise or defend legal claims or
- to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent.

Standard transfer agreements exist between the University and a number of international partners, the DPO should be consulted before any agreement to transfer personal data is made.

13. RETENTION OF DATA

We must not keep Personal Data in a form that allows Data Subjects to be identified for longer than needed for the legitimate educational/research or University business purposes or other purposes for which we have collected it. Those purposes include satisfying any legal, accounting or reporting requirements. Records of Personal Data can be kept for longer than necessary if anonynmised.

Staff should take all reasonable steps to destroy or erase from the University's systems all Personal Data that we no longer require in accordance with our Privacy Notices and the University's Record Retention schedule

14. SUMMARY

Compliance with Data Protection Legislation is the responsibility of all members of the University. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even a criminal prosecution.

You should contact the DPO if you have any questions about the operation of this policy or the application of Data Protection Law or if you have any concerns that this policy is not being

followed. In particular, you should contact the DPO if:

- you are unsure about what security or other measures you need to implement to protect Personal Data;
- there has been a Personal Data Breach;
- you are unsure on what basis to transfer Personal Data outside the EU;
- you need any help dealing with any rights invoked by a Data Subject;
- whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA or plan to use Personal Data for purposes other than for which it was collected;
- if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (such as overseas partners, agents, and organisations conducting surveys on the University's behalf).

APPENDIX A

Glossary

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Profiling: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in accordance with the GDPR. The University is the Data Controller of all Personal Data relating to it and used delivering education and training, conducting research and all other purposes connected with it including business purposes. .

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person appointed as such under the GDPR and in accordance with its requirements. A DPO is responsible for advising the University (including its employees) on their obligations under Data Protection Law, for monitor compliance with data protection law, as well as with the University's polices, providing advice, cooperating with the ICO and acting as a point of contact with the ICO.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive Personal Data: data revealing, racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership. It also includes the Processing of: genetic data; biometric data for the purpose of uniquely identifying a person; data concerning health; data concerning a person's sex life or sexual orientation; Personal Data relating to criminal convictions and offences including the alleged commission of offences or proceedings for offences or alleged offences.

Personal Data Breach: any breach of security resulting in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data, where that breach results in a risk to the Data Subject. It can be an act or omission.

Privacy by Design and Default: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Notices: separate notices setting out information that may be provided to Data Subjects when

the University collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee, student and donor privacy notices or the website privacy policy) or they may be stand-alone, one-time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties. In brief, it is anything that can be done to Personal Data from its creation to its destruction, including both creation and destruction.

Pseudonymisation or pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.