Data Protection Policy
2020 - 2025

Mission Statement

UCISA aims to be acknowledged by all stakeholders as the membership organisation that draws together and promotes the expertise of those leading and supporting digital transformation and services in educational institutions to support operational effectiveness, research, teaching and learning, and an excellent student experience.

Scope of Policy

1.1 UCISA is committed to full compliance with the General Data Protection Regulation (GDPR) (2016/679) and the Data Protection Act 2018, and recognises the responsibilities that these places on it to process and manage personal information in a fair and proper manner. UCISA has in place procedures to ensure practices exist to strike a balance between UCISA's needs and the individual's right to respect for their private life, confidentiality of data and the need to provide protection from unwanted or harmful uses of personal data.

1.2 Reference to 'staff' throughout this policy refers to employees, members of the Board of Trustee's as well as volunteer helpers of UCISA.

1.3 In processing and managing data UCISA complies with the principles of good practice noted in the Act. Specific procedures and processes are in place to ensure that the management of personal data adheres to these principles. The principles state that personal data shall be::

- processed lawfully, fairly and in a transpartent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

1.4 Rights under the Act are not subject to a minimum age requirement and are dependant on the lawful basis under which the data was originally collected .

2 Responsibilities

2.1 Ucisa is, as a corporate entity, the data controller under the Act. The Board of Trustee's is therefore ultimately responsible for implementation.

2.2 Ucisa has a designated Data Controller (Chief Executive Officer) who (either alone or jointly or in common with other persons) determine the lawful basis for how and why any personal data is, or is to be, processed with adherence to UCISA's Data Protection policy and procedures.

Ucisa has a designated Data Protection Officer who will advise on implications of Data Protection law and support the development of UCISA's Data Protection policy.

2.3 Ucisa has a valid notification in the data protection register that relates to processing information. This can be viewed at www.ico.org.uk It is the responsibility of the Data Controller to ensure the registration is checked and updated on a regular basis.

2.4 Data protection compliance is ultimately the responsibility of all UCISA staff. Individuals can be held legally responsible if they disclose personal information to any unauthorised third party. Serious breaches of data protection rules are considered to be a disciplinary matter.

2.5 In processing personal data staff are expected to:

- understand and adhere to the data protection principles set out in 1.2
- manage personal data in accordance with UCISA's Data Protection policy, other relevant policies and procedures and the guidelines in Appendix A.

2.6 All staff and (prospective and current) members are responsible for:

- checking that any personal information that they provide to UCISA is accurate and up to date
- informing UCISA of any changes to information which they have provided e.g. change of address
- checking the information that UCISA will send out from time to time, giving details of information kept and processed
- informing UCISA of any errors. UCISA cannot be held responsible for any errors unless the staff member or organisation member has informed UCISA.

3 Definition of Data

3.1 In the terms of the Act, data relates to an individual where the structure is such that information about the individual is readily accessed. The information may be held in manual form (e.g. as written notes relating to a person or as part of a filing system, including card index or filing cabinets structured by name, address or other identifier) or in a form capable of being processed electronically.

3.2 Personal data covers any data relating to a living individual (e.g. name, address, date of birth and any otherdigital information about that individual i.e. IP Addresses)that relate to a living person

Sensitive data form a subset of personal data and is considered to be "special category data" including the recording of information such as racial or ethnic origin, political opinions, religious beliefs, trade union membership, and health.. Sensitive data also specifically includes genetic and biometric data where processed to uniquely identify an individual.

Data about criminal convictions is also considered in a similar manner to that of sensitive data and can only be processed with both a suitable lawful basis and either legal or official authority to do so. Under the requirements of GDPR a comprehensive register of criminal convictions **cannot** be kept.

3.3 Lawfull processing of data must takes place whenever it is compiled, stored or otherwise operated upon. Giving and receiving personal references, producing agenda items or minutes for committees at which individuals are discussed as individuals, etc. Similarly, data about staff and applicants for posts are lawfully processed when they are committed to manual or electronic records held within UCISA for a specified purpose. The lawful basis under which processing takes place must be stated and the process itself documented.

4 Subject Consent

4.1 The Act does not allow an individual to prevent an organisation from making reasonable use of personal data in the interests of providing education or employment. For example, staff and members must expect certain information about them to be placed in the public domain. The agreement (of the data subject) to process staff or member data necessary in accordance with UCISA's contract to provide employment or education will be gained at application.

4.2 Sometimes it is necessary to process information about a person's physical and mental health, race or ethnicity, sexual life, political or religious views and trade union membership details. This may be to ensure UCISA is a safe place for everyone, to assess suitability for employment or to operate other organisation policies, such as the sick pay policy or single equality policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and members will be asked to give express consent for UCISA to do this however where this is not given UCISA may consider the application of the lawful basis of vital interest in order to protect an individual.

5 Rights to access information

5.1 Subject to a limited number of statutory restrictions, an individual or data subject (who could, for example, be a past or present member, a past or present member of staff or a current or previous applicant for a post) has a right to gain access to information that is kept about them.

5.2 A request to gain access should be made either orally or in writing, together with proof of identity, where relevant, to the Chief Executive Officer. This provision allows for an individual to verify the lawfulness of the processing. There is no charge for this service

When a request is considered to be manifestly unfounded or repetitive, or when further copies are requested for the same information may be refused or a "reasonable fee" will be charged. The fee will be based on the administrative cost of providing the information.

5.3 Ucisa aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory period of one month from receipt for all information. This may be extended by a further two months if the request is complex or numerous and if this is the case the requestor will be advised of this within one month of an enquiry being made (from receipt) has been received and they will informed why this is necessary.

5.4 In certain circumstances information released could include information that enables a third party to be identified. In such circumstances UCISA will redact the information which identifies the third party.

6 Retention of Data

6.1 Basic details will be retained until notified. These will include:

Organisational Representative

- Title
- Name
- Organisation
- Job Title
- Department
- Email address
- Telephone Number

Members

- Name
- Organisation
- Organisation Address
- Department
- Job Title
- Email address
- Telephone Number
- Subject of Interest
- UCISA Group Membership

Events (Details will be retained for 30 days after the event)

- Name (selected from a list)
- Dietary requirements
- Details of Allergies
- Special Assistance Requirements

6.1.3 All personal database records and personal documents (with the exception of information detailed in 6.1.1) on employees will be kept for a maximum of seven years from the date that they left UCISA after which they will be destroyed and/or deleted, e.g., references, disciplinary records.

6.1.4 Application data of unsuccessful applications for employment will be held for no longer than required (normally 1 year after employment for the post is taken up), unless a data subject has exercised their right to erasure before this date.

6.2 Staff

6.2.1 Basic details will be retained electronically indefinitely. These will include:

- name
- (last known) postcode(reduced to first component i.e. RM11)
- date of birth
- dates employed
- posts held

6.2.2 All personal database records and personal documents on staff will be kept for a maximum of seven years from the date that they have left UCISA, after which they will be destroyed and/or deleted.

6.2.3 Where necessary, information in respect of pensions, taxation, potential or current disputes or litigation regarding the employment, health and information required for job references will be kept for longer periods. (See Appendix B)

6.2.4 Data on unsuccessful external applicants and unsolicited or speculative applicants for employment will be retained for a maximum of one year (from the date on which the application was made) unless the data subject has exercised their right to erasure.

7. Breach Notification

7.1.1 A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

7.1.2 When a breach occurs **and it is likely to result in a risk to the rights and freedoms of invidiuals** then it is necessary to notify the Data Protection Officer (DPO) as soon as the breach is identified. If necessary the DPO will contact the relevant supervisory authority (Information Commissioners office) **within 72 hours** of becoming aware of the breach. If the breach is sufficiently serious then the DPO will inform the public of the breach without undue delay. If the risk is considered to be a "high risk" to the rights and freedoms of an individual then the individuals will be contacted directly.

7.1.3 A breach notification must contain the following information:

- The nature of the personal data breach including where possible:
  - The categories and approximate number of individuals concerned; and
  - The categories and approximate number of personal data records concerned.
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and where appropriate, of measures taken to mitigate any possible adverse effects.

Where it is deemed necessary the DPO will provide the ICO with this information. This information will also be recorded in the Breach Register.

7.1.4 Failure to notify of a breach when required to do so may result in a fine of up to €10 million or 2% if global turnover, which ever is the greater.

8. Transfer of Data

8.1.1 Transfer of data to another organisation can only take place where the organisation receiving the the personal data has provided adequate safeguards such as:

- A legally binding agreement between public authorities or bodies;
- Provisions inserted in to administrative arrangements between public authorities or bodies.

9. Appendices

A. General guidelines
B. Retention of Records containing Personal Data (currently under review).
C. Clear Desk Policy

10. Further Guidance

Information Commissioners' website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Appendix A

General Guidelines

1. Storing Personal Data

Personal data must be held securely. In the case of manual data this could be in locked filing cabinets, locked cupboards or rooms with access restricted to named individuals or categories of individual only. In the case of electronic information, access must be subject to reasonable controls including passwords and restricted access rights. Reasonable steps must be taken to detect and prevent unauthorised access. Regular backups should be taken to ensure that important data cannot be lost.

2. Disclosing Personal Data

Personal data should not generally be disclosed to third parties without the permission of the individual concerned. This covers both intentional disclosure and any disclosure that may happen by accident, for example someone having oversight of a monitor on which data is displayed. In this context, 'third parties' includes family members, friends, local authorities, government bodies and the police unless disclosure is exempted by the 2018 Act or by other legislation. Under certain circumstances, data may however be released. Note that among other circumstances the Act permits release of data without express consent:

- for the purpose of protecting the vital interests of the individual (e.g. release of medical data where failure to do so could result in harm to, or the death of, the individual)
- for the prevention or detection of crime
- for the apprehension or prosecution of offenders
- for the assessment or collection of tax
- where the disclosure is required whether as a statutory requirement or in response to a court order.
- Where there is a legally binding agreement between public authorities or bodies.

Most bodies that request personal data in such circumstances should be able to provide documentary evidence to support their request. For example, many police forces have a specific procedure for requesting information in support of an ongoing investigation. The absence of such documentation, court order or a warrant may justify refusal to disclose personal data. Where there is a statutory obligation to disclose, the disclosure must be made. Requests of this nature should be passed to the Chief Executive Officer.

UCISA will obtain the **consent** of data subjects, i.e. staff, members and others, where non-sensitive personal data (including photographs) is to be used on UCISA internet, intranet web pages and in other publications where such use is not for the purposes of the normal organisational functioning and management of the institution for example general marketing purposes including publicity photographs, press releases, prospectus etc.

As a rule, personal or sensitive data should not be disclosed without the express **consent** of the individual concerned. Telephone disclosure is discouraged and is generally unsatisfactory, as verification of such details (and the identity of the enquirer) can be difficult.

For example, a member's address, telephone number or e-mail should not be given to a telephone enquirer, even if the enquirer claims to be a close relative or friend. If a phone call is received from a third party requesting information on a member of staff or member, information about the individual should not be disclosed, however hard the caller may press, without the express permission of the individual concerned. Offer to attempt to contact the individual concerned and take details of the request for information, including the caller's number. If necessary, ask them to put their request in writing and offer to accept a sealed envelope to forward to the individual concerned. Follow similar guidelines when dealing with written requests for information.

3. Protecting Third Parties

In meeting a data subject access request, it is important that personal data relating to other identifiable individuals mentioned in the documents (e.g. other staff ormembers) should not also be revealed unless permission for disclosure is given by the individual(s) concerned. Thus, a data subject enquirer has the right to see notes or comments relating to them that are held by UCISA in manual or electronic form, but the identity of the individual(s) who made those comments **must** be redacted.

4. Disposal of Personal Data

Personal data should be disposed of when no longer needed for the effective functioning of UCISA and its members (see Appendix B for period of retention for records). The method of disposal should be appropriate to the sensitivity and nature of the data. Data on paper must either be (personally) shredded or placed in a secure disposal bin designated for that purpose and electronic data be permanently destroyed as appropriate. Note that 'deleting' a computer file does not equate to destroying the data: such data can often be recovered.

5. Applications for Employment

Notes made in the course of interviews constitute individual data and are therefore subject to access under the Act. They should be fair, reasonable and defensible. Interview notes relating to successful applicants may be retained while the individual is a member of UCISA, and hence be disclosable in response to a data subject request. Interview notes and all personal data relating to unsuccessful external applicants will be retained for a maximum of one year after it has become clear that the individual will not be appointed or admitted to UCISA, unless the data subject has exercised their right to be erased.

Appendix B

Retention of Records containing Personal Data

Statutory retention periods:

Type of Record	Statutory Retention Period	Statutory Authority
Employee Contact Details	5 Years post employment	**HMRC**
Employee Bank Details	5 Years post employment	
Employee Pension Details	75 Years post employment	**HMRC**
Employee Tax Details	6 Years post employment	**HMRC**
Employee Pay Details	6 Years post employment	**HMRC**
Employee Annual Leave Details	6 Years post employment	
Employee Sick Leave Details	6 Years post employment	
Employee Performance Details	6 Years post employment	
Employee Qualifications	6 Years post employment	
Employee Work History	6 Years post employment	
Employee Ethnicity	6 Years post employment	
Employee Disability Details	6 Years post employment	

Recommended retention periods (i.e. where no statutory retention periods exist. Sources: ICO and CIPD)

Type of Record	Suggested Retention Period	Reason for Length of Period
Applicant Contact Details	6 months post application	
Employee Qualifications	6 months post application	
Employee Work History	6 months post application	
Employee Ethnicity	6 months post application	
Employee Disability Details	6 months post application	
Member Name	1 year after leaving post	
Member Contact Details	1 year after leaving post	
Member Job Title	1 year after leaving post	
Member Department	1 year after leaving post	
Event Member Name	30 days after event	
Event Dietary Requirements	30 days after event	
Event Allergies	30 days after event	
Event Special Assistance	30 days after event	

Appendix C

Clean Desk Policy

Overview

To improve the security and confidentiality of information, UCISA will be adopting a 'Clean Desk Policy' for all desks, computer workstations and printers.

This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device, is properly locked away or disposed of when a desk, workstation or printer is not in use. This policy will reduce the risk of unauthorised access, loss of, and damage to information during and outside of normal working hours or when desks, workstations and printers are left unattended.

A Clean Desk Policy is an important security and privacy control and necessary for compliance with GDPR (General Data Protection Regulations).

Scope

This policy applies to all permanent, temporary, and contracted staff working at UCISA.

Policy

Whenever a desk or workstation is unoccupied for an extended period of time the following will apply:

1. All sensitive and confidential paperwork must be removed from the desk and locked in a drawer or filing cabinet. This includes mass storage devices such as CDs, DVDs, and USB drives.
2. All waste paper which contains sensitive or confidential information must be placed in the designated confidential waste bins or personally shredded. Under no circumstances should this information be placed in general waste bins.
3. Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the work day.
4. Laptops, tablets, and other hardware devices must be removed from the desk and locked in a drawer or filing cabinet.
5. Keys for accessing drawers or filing cabinets should not be left unattended at a desk.
6. Printers and other transmission devices should be treated with the same care under this policy:
    a. Any print jobs containing sensitive and confidential paperwork should be retrieved immediately. When possible, a "Locked Print" functionality should be implemented and used.
    b. All paperwork left over at the end of the work day must be properly disposed of.

Policy Identification Number	
Ucisa/USL policy 02 of 2020	
Policy Title	
Data Protection Policy 2020-2025	
Policy Enabling Owner	**Responsible for Implementation**
CEO	All staff
Approving Body	**Date of Approval**
Board of Trustees	March 2020
Last Reviewed	**Review Due Date**
	July 2021
Publication of Policy *(tick as appropriate)*	
For public access online (internet)? ☒	**For staff access only (intranet)?** ☒
Queries about this policy should be referred to	
Deborah Green - ceo@UCISA.ac.uk	