HERTS SU

Hertfordshire Students' Union

DATA PROTECTION POLICY

1. Introduction

The Student's Union is committed to all aspects of data protection and takes seriously its duties, and the duties of its employees, under the General Data Protection Regulation (GDPR). This policy sets out how the Student's Union deals with personal data, including personal files, students' data and data subject access requests, and employees' obligations in relation to personal data.

2. Data Controller

Hertfordshire Students' Union is a data controller. The Union processes personal information relating to students, staff and visitors. The Board of Trustees delegates day to day responsibility for implementing this policy and related procedures to key personnel within the Union. The Students' Union and its subsidiaries are registered as a Data Controller with the Information Commissioner's Office (ICO) and renews these registrations annually.

3. Data Protection Officer

The General Manager is the Students' Union Data Protection Officer and is responsible for the implementation of this policy. If employees have any questions about data protection in general, this policy or their obligations under it, they should direct them to the General Manager.

4. Data protection principles

The Union processes personal data in accordance with the following data protection principles:

- Processing personal data lawfully, fairly and in a transparent manner.
- Collecting personal data only for specified, explicit and legitimate purposes.
- Processing personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Keeping accurate personal data and taking all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Keeping personal data only for the period necessary for processing.
- Adopting appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

The Union tells individuals the reasons for processing their personal data, how it uses such data and the legal basis for processing in its privacy notices. It will not process personal data of individuals for other reasons.

Personal data is held in the individual's personal file (in hard copy or electronic format, or both), and on IT systems. The periods for which the Trust holds HR-related personal data are contained in the Data Retention Policy.

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely. For example, we will shred paper-based records, and override electronic files.

We may also use an outside company to safely dispose of electronic records.
The Union maintains a record of its processing activities in respect of HR-related personal data in accordance with the requirements of the General Data Protection Regulation (GDPR).

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as HMRC so that they are able to meet their statutory obligations.

More information can be found within the Union's Privacy Notices.

5. Personal data

5.1 The GDPR applies to information that constitutes "personal data". Information is "personal data" if it:

- identifies a person, whether by itself, or together with other information in the organisation's possession, or is likely to come into its possession; and
- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature.

5.2 Consequently, automated and computerised personal information about individuals held by the Union is covered by the policy. Personal information stored physically (for example, on paper) and held in any filing system is also covered. In addition, information recorded with the intention that it will be stored in a relevant filing system or held on computer is covered.

6. "Sensitive personal data"

6.1 "Sensitive personal data" is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the
- disposal of such proceedings or the sentence of any court in such proceedings.

6.2 The Students' Union will not retain sensitive personal data without the express consent of the employee in question.

6.3 The Students' Union will process sensitive personal data, including sickness and injury records and references, in accordance with the data protection principles. If the organisation enters into discussions about a merger or acquisition with a third party, the organisation will seek to protect employees' data in accordance with the data protection principles.

7. The use of personal information

7.1 The policy applies to personal information that is "processed". This includes obtaining personal information, retaining and using it, allowing it to be accessed, disclosing it and, finally, disposing of it.

8. Personnel files

8.1 An employee's personnel file is likely to contain information about his/her work history with the Students' Union and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

8.2 There may also be other information about the employee located within the Students' Union, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

8.3 The Students' Union may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, the Students' Union will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the Students' Union will inform employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the Students' Union who will have access to that information and the security measures that the Students' Union will put in place to ensure that there is no unauthorised access to it.

8.4 The Students' Union will ensure that personal information about an employee, including information in personnel files, is securely retained. The Students' Union will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary. For guidance on Retention of date see Appendix One.

8.5 8.5 The Students' Union provides training on data protection issues to all employees who handle personal information in the course of their duties at work. The Students' Union will continue to provide such employees with refresher training on a regular basis. All employees of the Students' Union have confidentiality clauses in their contracts of employment.

8.6 8.6 Where laptops are taken off site, employees must follow the Students' Union relevant policies relating to the security of information and the use of computers for working at home/bringing your own device to work.

9. Individual rights

9.1 As a data subject, you have a number of rights in relation to your personal data.

9.2 Subject access requests

You have the right to make a subject access request. If you make a subject access request, the Union will tell you:

- whether or not your data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from you;
- to whom your data is or may be disclosed;
- for how long your personal data is stored;

- your rights to rectification or erasure of data, or to restrict or object to processing;
- your right to complain to the Information Commissioner if you think the Union has failed to comply with your data protection rights; and
- whether or not the Union carries out automated decision-making and the logic involved in any such decision-making.

The Union will also provide you with a copy of the personal data undergoing processing.

To make a subject access request, you should send the request to the General Manager.

In some cases, we may need to ask for proof of identification before the request can be processed. We will inform you if we need to verify your identity and the documents we require.

We will normally respond to a request within a period of one month from the date it is received.

If a subject access request is manifestly unfounded or excessive, for example is a repeat of a previous request, we are not obliged to comply with it. Alternatively, we can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request.

9.3 Other rights

You have a number of other rights in relation to your personal data. You can require the Union to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if your interests override our legitimate grounds for
- processing data (where we rely on legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about
- whether or not the individual's interests override our legitimate grounds for processing data.

To ask the Union to take any of these steps, you should send the request to the General Manager.

10. Data sharing

The Union will not transfer data to countries outside the EEA.

11. Monitoring

11.1 11.1 The Students' Union may monitor employees by various means including, but not limited to, recording employees' activities on CCTV, checking emails, listening to voicemails and monitoring telephone conversations. If this is the case, the Students' Union will inform the employee that monitoring is taking place, how data is being collected, how the data will be securely processed and the purpose for which the data will be used. The employee will usually be entitled to be given any data that has been collected about him/her. The Students' Union will not retain such data for any longer than is absolutely necessary.

11.2 In exceptional circumstances, the Students' Union may use monitoring covertly. This may be appropriate where there is, or could potentially be, damage caused to the Students' Union by the activity being monitored and where the information cannot be obtained

effectively by any non-intrusive means (for example, where an employee is suspected of stealing property belonging to the Students' Union). Covert monitoring will take place only with the approval of the General Manager.

12. Employees' obligations regarding personal information

12.1 Individual responsibilities

You are responsible for helping us keep your personal data up to date and should notify the Union of any changes promptly.

You may have access to the personal data of students or other individuals in the course of your job role.

Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the Union) who have appropriate authorisation;
- to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction);
- not to use emails to send any personal data outside of the SU, you can use the secure data transfer system (exchange file) accessible at https://www.exchangefile.herts.ac.uk ;
- not to remove personal data, or devices containing or that can be used to access personal data, from the Union's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device; and
- not to store personal data on local drives, USB sticks, moveable data or on personal devices that are used for work purposes.

12.2 Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under our disciplinary procedure or Code of Conduct. Significant or deliberate breaches of this policy or of the relevant sections of the Code of Conduct, such as accessing personal data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

13. Review of procedures and training

13.1 The Union will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that he/she would benefit from refresher training, he/she should contact the HR Department.

13.2 The Union will review and ensure compliance with this policy at regular intervals.

HERTS SU

APPENDIX ONE

Retention of data

The following list shows different types of data and the length of time they will be kept for. For data not contained on this list, the Data Controller or the Human Resources Manager should be consulted about the length of its retention.

Descriptions of Data	Retention Period	Recommended Action Following Retention
Personnel files, training records	6 years after employment ceases	Delete electronic data files Shred hard copy files
Notes of disciplinary and grievance hearings	6 years after employment ceases	Delete electronic data files Shred hard copy files
Application forms and interview notes for unsuccessful candidates	Min 6 months to 12 months	Delete electronic data files Shred hard copy files
Facts relating to redundancies	6 years from date of redundancy	Delete electronic data files Shred hard copy files
Income tax and NI returns and related correspondence with Inland Revenue	6 years	Delete electronic data files Shred hard copy files
Parental leave, Statutory Maternity Pay calculations and records	6 years	Delete electronic data files Shred hard copy files
Statutory sick pay records and calculations	6 years	Delete electronic data files Shred hard copy files
Wages and salary records	6 years	Delete electronic data files Shred hard copy files
Accident books, records and reports of accidents	3 years after date of last entry	Delete electronic data files Shred hard copy files
Health records	During employment	Delete electronic data files Shred hard copy files
Health records where reason for termination of employment is connected with health	3 years	Delete electronic data files Shred hard copy files

HERTS SU

Descriptions of Data	Retention Period	Recommended Action Following Retention
Medical records kept by reason of Control of Substances hazardous to Health	40 years	Delete electronic data files Shred hard copy files
Bans	Life	
Membership information, including society/sports/volunteers/ media	Up to 3 years from the date of membership	Delete electronic data files Shred hard copy files
Suppliers' documentation and records	6 years after the end of the financial year	Delete electronic data files Shred hard copy files
Advice Casework	7 years from the date of last contact	Delete electronic data files Shred hard copy files

HERTS SU

APPENDIX TWO

GENERAL GUIDANCE

The following information is for guidance only. If you are in any doubt about use, collection, storage or disclosure of personal data you should consult the Data Controller or the Human Resources Manager.

1. Disclosure of personal data

You should not disclose personal data to a third party unless:

- The disclosure is covered by the list in Appendix One.
- You have the consent of the data subject.
- The disclosure is in the interests of the person in an emergency or similar circumstance i.e. the person is taken to hospital and is known to be pregnant or have a condition such as diabetes or epilepsy when you would be expected to inform the hospital.

If you receive a request from the police for information you should refer them to the General Manager or, in his absence, another Senior Manager.

If you are in any doubt, do not disclose the information but seek guidance from the Data Controller, a Senior Manager or the Human Resources Manager.

2. Dealing with personal data

You must take reasonable steps to ensure the security of Personal Data and ensure:

- Computers and not placed in a public area where unauthorised persons can read the
- screen.
- Personal files are kept in locked cabinets and not on desks, particularly overnight.
- Lock your workstation when you leave it.
- USB sticks should be used minimally, should be kept locked away and not left lying around.
- Unwanted confidential paperwork should be shredded.
- Highly sensitive material should be depersonalised or coded where practicable.
- Computer passwords should be changed regularly, not shared and not easy to imitate.
- Permissions to systems, folders etc are properly set to prevent unauthorised access and are updated when staff move into different roles.
- Unwanted data on CD's or portable hardware should be erased or overwritten.
- Where data has been downloaded onto computers, it should not be copied and used elsewhere and must not be kept longer than necessary.
- Avoid taking personal information home with you.
- If you need to save personal data onto a laptop or removable storage then ensure it is encrypted.

When dealing with personal data you should ask yourself the following:

- Do you need to record the information?
- Is the information "sensitive data"?
- Do you have the data subject's consent, i.e. is it on the list in Appendix One?

- Are you authorised to control, store or process personal data?
- Have you checked that the data is accurate?
- Is the data secure?

3. Writing notes about individuals

When writing notes about individuals you should ensure that:

- Comments are fair, accurate and justifiable
- You would be comfortable showing the information to the data subject.

4. Writing references

References can no longer be guaranteed to be confidential. When writing a reference you must ensure that you:

- Confirm the accuracy of or provide accurate information
- Differentiate between fact and opinion
- Express only fair and justifiable opinions, based on first-hand experience. Avoid ambiguity.
- Be fair and accurate

All copies of references should be forwarded to the Human Resources Manager so that they can be placed on the personnel file.

APPENDIX THREE

USES OF PERSONAL DATA

The following is a list of purposes for which Hertfordshire Students' Union may process personal data. The processing of some data may continue after the people have ceased to be employed by the union.

By signing this policy staff agree to the union processing their data for the following purposes.

1. Payment of salary, pension, sickness benefit or other payments due under the contract of employment.
2. Performance related pay or promotion exercises
3. Monitoring absence or sickness under absence control or capability policies.
4. Training and development purposes
5. Management planning
6. Providing and obtaining references and consultation with external agencies including police checks where necessary for the purposes of employment.
7. Negotiations with Trade Unions or other staff representatives.
8. Administration of the union's policies and procedures.
9. Compliance with the Disability Discrimination Act
10. Compliance with other statutory requirements to provide information about staff including statistical returns to external bodies
11. Administration of the union's disciplinary and grievance procedures
12. Production of published staff lists including e mail and telephone directories for internal and external use.
13. Production of ID cards
14. Monitoring the use of the union's resources
15. Use of CCTV to protect staff, customers and property