# Data Protection Policy Aston Students’ Union (ASU)



Contents

[Definition of data protection terms 2](#_Toc514421195)

[Policy Statement 3](#_Toc514421196)

[Principles of Data Protection ASU adhere to: 3](#_Toc514421197)

[The GDPR provides the following rights for individuals: 4](#_Toc514421198)

[Accountability and Transparency 5](#_Toc514421199)

[Data Processing within ASU 5](#_Toc514421200)

[Data Usage: Summary 7](#_Toc514421201)

[Data Protection Impact Assessment 8](#_Toc514421202)

[Data Sharing, Data Security and Disposal 8](#_Toc514421203)

[Requests for Information 9](#_Toc514421204)

[Complaints 9](#_Toc514421205)

[Appendix A: Data Retention Schedule: Data Retention for Charities 10](#_Toc514421207)

[Appendix B: Data Retention Schedule: HR/Finance/People related 12](#_Toc514421208)

[Appendix C: Data Retention Schedule: Data Retention for Aston Students’ Union Activity 14](#_Toc514421210)

[Appendix D: Guidelines for staff including Staff Checklist for Recording Data 15](#_Toc514421211)

[Appendix E: Data Protection Impact Assessment 16](#_Toc514421212)

# Definition of data protection terms

**“Data”** is information that is stored electronically, on a computer, or in certain paper-based filing systems.

**“Data subjects”** for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

**“Personal data”** means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal and opinions and comments recorded in our files).

**“Data controllers”** are the people or organisations, which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Data Protection Act. We are the data controller of all personal data used in our organisation.

**“Data users”** include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

**“Data processors”** include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers that handle personal data on our behalf.

**“Processing”** is any activity that involves use of the 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 transferring personal data to third parties.

**“Sensitive personal data”** includes information about a person’s racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Generally speaking, sensitive personal data should only be processed with the explicit consent of their subject, or where required by law.

# Policy Statement

Aston Students’ Union (ASU) recognises that our members, and others, have the right to know what data we hold about them, and that any data held is in compliance with the Data Protection Act (the Act). We process personal information about our members and staff in accordance with the six principles of the Data Protection Act.

## Principles of Data Protection ASU adhere to:

1. **Children’s Personal Data**

When services are offered directly to a child, an organisation must ensure that their privacy notice is written clearly and in way that a child can understand.

1. **Legitimate use of Personal Data**

Personal Data can only be obtained for the specific, explicit and legitimate purposes and can then only be processed for that purpose. It cannot be processed for another purpose without the further consent from the data subject. Personal Information must be processed in line with the data subject’s rights, under the Act.

1. **Data Minimisation**

Personal data collected on an individual should be adequate, relevant and limited to what is necessary. In other words, no more than the minimum amount of personal data should be kept for specific processing.

1. **Accuracy**

Personal information must be accurate and up to date.

1. **Storage of Data and its limitation**

Personal information must not be kept for longer than is necessary.

1. **Security of Data**

The storage of personal information must be secure; appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

# The GDPR provides the following rights for individuals:

|  |  |  |
| --- | --- | --- |
| **GDPR Right** | **What the laws Says** | **Aston Students’ Union position** |
| **The right to be informed** | Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR. | When students enrol with the university they are made aware of what data is collected and processed and how this is shared with the Students’ Union  Student who actively engage with the Students’ Union are further informed about how their data is processed |
| **The right of access** | Individuals have the right to access their personal data. | Students can ask to see their data at any time and the SU will respond within one month of the request |
| **The right to rectification** | The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. | ASU will try is best to ensure that the data held is accurate. Over time and in some cases, students will be able to access their own ‘online profiles’ to ensure accuracy  They can at any time request that their data is rectified |
| **The right to erasure** | The GDPR introduces a right for individuals to have personal data erased. | Students will be able to request this at any time. In some circumstances it may mean that they are unable to participate in all or some union activity, including voting in the elections and being an active committee member of a club or society |
| **The right to restrict processing** | Individuals have the right to request the restriction or suppression of their personal data. | The Union would restrict the processing of data as requested. This might be for example not including all Union activity in the HEAR report |
| **The right to data portability** | The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. | If asked the Union would provide the data. This would be in electronic format |
| **The right to object** | The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. | We recognised that in terms of direct marketing purposes individuals have an absolute right to stop their data being used |
| **Rights in relation to automated decision making and profiling** | The GDPR has provisions on automated individual decision-making and profiling | Currently the Union makes no decision about individuals based on automated consideration of their data |

# Accountability and Transparency

This policy and the body of work it represents demonstrates ASU compliance with the data protection principles and that the responsibility rests with the origination as a data controller and data processor.

The Chief Executive is responsible for the general development, promotion and adherence to this policy, and ultimately responsible for compliance by all elected officers, staff and volunteers. The Chief Executive is also the Data Protection Officer and can be contacted at this address for any data related questions [m.mcloughlin@aston.ac.uk](mailto:m.mcloughlin@aston.ac.uk)

The Act does not specify periods for the retention of personal data. ASU considers the Data Protection Principles, business needs, legitimate interests and any professional and legal guidelines, in determining how long it stores specific types of data. A Data Retention Schedule is attached as Appendix A, B and C taking into account retention schedules for charities, legal/Finance/HR legislation and needs of the organisation.

All elected officers, staff and volunteers who process personal data are expected to understand and adhere to this policy and the Data Protection Principles set out in the Act. All staff and officers will undertake the GDPR training as supplied by Aston University’s Virtual Learning Environment (VLE).

Staff and officers should refer to the Staff Checklist for Recording Data in their day-to-day work, and this is attached as Appendix B.

ASU will use, when appropriate and proportionate, Data Protection Impact Assessment (Appendix D) and ensure that the collection and use of data falls within the law and is for the legitimate needs of the organisation.

The Chief Executive is responsible for ensuring that adequate and appropriate knowledge and competence for good data protection exists across the organisation. The Senior Management Team are responsible for the oversight of relevant data protection issues and should raise these for discussion, resolution and communication across ASU.

Our responsibilities will be met by making available this policy and procedures to all colleagues, compulsory training and development for new elected officers, staff and volunteers, and ongoing training and development for colleagues with access to sensitive data, and with management responsibility.

It is the belief of ASU that these measures will uphold the protection of personal data and both demonstrate and ensure compliance with the Act.

# Data Processing within ASU

‘Processing’ is anything done with personal data including collection, storage, disclosure, use and deletion; this section sets out the most common ways in which ASU processes data. Any non-standard processing of data must be checked with the Chief Executive to ensure that it is consistent with this Data Protection Policy.

The following is a non-exhaustive list of the ways and manner in which the Union collects and processes data about its staff and student members

**Students as Member of the Students’ Union**

Students have the right to opt-out of membership of ASU and give express consent to personal and sensitive data being collected and processed. This information is shared between Aston University and ASU under the terms of a Memorandum of Understanding, with specific reference to data sharing.

A key part of membership is regular communication sent to students’ university email addresses, that outlines key events and activities that are taking place to allow the organisation to achieve its charitable aims and to contact students with information, which may be of value to them.

**Students, Officers and Staff as Employees**

All staff consent to ASU using their data when they start employment; the notification and request for consent will form part of their terms and conditions of employment. The data collected includes sensitive personal data, such as banking, health, disciplinary and diversity information. Staff should manage their own profile and information accordingly via the Aston CORE HR system.

ASU will not disclose a confidential reference, given to a third party for the purposes of education, training, employment or the provision of any service, to the person that the reference is about. The reference could, however, become accessible to the subject of the reference from the person to whom it is sent.

During the time spent as an employee (the career of the staff members) the Union will collect and process other data related to the individuals this includes but is not limited to performance appraisals, financial records (expenses), disciplinary investigations and outcomes (where relevant).

References for elected officers and staff may only be authorised by the line managers with support from the Senior Management team.

ASU would not usually complete a reference for a volunteer but, should this occur, will store any reference within our human resources files.

**Students as clients in the Advice and Representation Centre (ARC)**

ASU processes sensitive data on behalf of clients who use our Advice and Representation Centre. Clients are asked to give informed consent to the slightly different ways in which we process, share, secure and dispose of their data by signing a specific consent form. The ARC staff team reviews this process annually, using guidelines suggested by Advice Quality Standard AQS[[1]](#footnote-1). The full suite of ARC polices are available from the ARC reception desk.

**Students as Members of Clubs and/or Societies**

ASU collects and processes information in relation to whether students join clubs and societies and the nature of their involvement (committee member or standard member).

Further data and information will be collected on committee members who have a responsibility to run the clubs and societies including but not limited to (Financial information to manage their accounts, training records, contact/address to ensure a Duty of Care).

**Students as Course Reps**

ASU and the University will share data on which students are course reps, the meetings they may attend and the outcomes of those meetings.

**Students and Staff as Customers**

If students choose to buy items online or in the shop/bar with their debit card the Union will collect further relevant information.

**Suppliers/Stakeholders**

Information relating to suppliers or other stakeholders, including contact details, bank account details and invoices, is stored on a secure system in the finance office and IT servers.

**Website and Membership Administration**

ASU has a significant operational relationship with Membership Solutions Limited (MSL). This company provide the membership management tools and website of the Students’ Union. A key element to success is their ability to store data, which ASU and its active volunteers then use to carry out their day to day tasks. MSL’s approach to Data Protection can be found here: <https://www.ukmsl.com/news/gdpr/>

# Data Usage: Summary

A summary of how data is used is included in the table below. This is not an exhaustive list and ASU reserves the right to use data in ways other than those listed below, but always within the confines of this policy. This includes details of the Processing of Personal Data as required by Article 28(3) GDPR:

|  |  |
| --- | --- |
| **Data Required** | **Purpose** |
| **Student ID Number** | to identify membership; to run elections (including voting and analysis of results) |
| **Title, Forename, Middle Name and Surname** | to identify member and carry out SU activities as identified |
| **Emergency Contact** | to be used for emergency contact only |
| **Contact Details (Address/Email/Telephone):** | to communicate with members as and when relevant and timely |
| **Date of Birth:** | to identify member, to identify whether they are a mature student and to identify potential need of membership as well as target communications |
| **Nationality:** | to analyse service provision, membership need and target communications |
| **Home, EU or International Student Status;**  **Enrolment Status:**  **Programme of Study/Mode of Study/Location of Study/Mode of Attendance:** | to analyse service provision and membership need as well as target communications; to allow for course rep elections and support |
| **School and Department/Year of Study:** | to analyse service provision and membership need as well as target communications; to allow for online elections for course reps and monitoring of the reps scheme performance |
| **Grades and Grades pending:** | to deal with academic enquiries and support the ARC service |
| **Assessments a student is registered on and the number of attempts they have had at each assessment:** | to deal with academic enquiries within the ARC and deal with any issues surrounding these |
| **Full Demographics: Gender, Ethnicity, Religion, Disability** | segmentation data required for cultural inclusion, targeting of services/events to relevant students and for reporting purposes |
| **Bank and Financial Details** | To process expenses payments, to allow payments to be made in the shops and commercial outlets |
| **Details of Guest speakers (contacts, social media profiles)** | To allow the Union to carry outs its due diligence under the PREVENT legislation and University PREVENT policy |
| **Details related to driving licences and offenses** | To allow certain students the ability to drive the Union vehicle fleet |
| **Data in relation to students’ engagement in Union decision making structure** | Attendance at meetings, policy submissions, voting records, candidacy and elected roles |
| **Engagement in ASU (Committee position, accolades, positions of responsibility)** | This data is required for the legitimate needs of the day-to-day business and at the end of the year is shared with the University for the purposes of populating the Higher Education Achievement Record (HEAR) |

# Data Protection Impact Assessment

Where ASU is beginning a new project or activity or where a project is up for a regular review a Data Protection Impact Assessment will take place. This is a sense check of either current data protection practices or potential new ones. The process will broadly follow the guidelines below:

1. **Identify the need for the DPIA** – determine whether the inherent risks of the processing operation require you to undertake a DPIA.
2. **Describe the information flow**– be able to describe how the information within the processing operation is collected, stored, used and deleted.
3. **Identify privacy** **and related risks** – catalogue the range of threats, and their related vulnerabilities, to the rights and freedoms of individuals whose data you collect and/or process.
4. **Identify and evaluate privacy solutions** – for each identified risk to the personal data, make a ‘risk decision’, i.e. whether to accept or reject the risk, whether to transfer it or take steps to reduce the impact or likelihood of the threat successfully exploiting the vulnerability.
5. **Sign off and record the DPIA outcomes**– record the outcomes of the DPIA (steps 1-4) in a report that is signed off by whoever is responsible for those decisions. Where a high risk has been identified, the organisation must submit the DPIA to the regulatory authority for consultation.
6. **Integrate the DPIA outcomes into the project plan**– you will need to continually refer to the DPIA in order to ensure that it is being followed and that its responses to the risks have been implemented effectively.

A copy of the Data Protection Risk Assessment is included in Appendix D

# Data Sharing, Data Security and Disposal

In order to prevent unauthorised processing, or accidental loss, damage or destruction, paper records that hold personal data are stored in locked filing cabinets, and electronic records are stored in drives, applications and servers that are securely managed.

We will only share data across different business functions, and colleagues at ASU when it is required in order to perform necessary work.

We sometimes share data with external partners, such as Aston University and the National Union of Students, under specific Data Sharing Agreements. As far as possible data is transmitted solely over a secure network connection, and the transmission of printed data through the post, or through independent electronic devices is strongly discouraged. ASU uses a secure network system with fully managed access control, back-up and recovery processes in place, and this is managed by Aston University.

Data is retained and disposed of according to need and in conjunction with the Data Retention Schedule. At the end of the retention period we dispose of, or destroy all data, confidentially where necessary; we shred paper files and delete electronic data from central systems.

# Requests for Information

The Act gives any individual, as a ‘data subject’, the right to receive details of personal information concerning them that is stored and processed by ASU. The Act requires us to present data within 40 days, but we will always try to meet our responsibility as soon as possible.

We welcome requests to access data that we hold, but we will need to authenticate the identity of any individual who makes a Subject Access Request. We therefore ask for any Subject Access Request to be sent to the Chief Executive through [m.mcloughlin@aston.ac.uk](mailto:m.mcloughlin@aston.ac.uk). We may need to ask for more information before we can process the request and locate the data.

When the Chief Executive receives a Subject Access Request, they will ask all Managers to search the data that they hold and provide the information necessary.

Requests for information about another person from a third party (including, for example, other ASU members, family, local authorities or the police) should be referred to the Chief Executive.

The Policies Manual for the Advice Service has some specific notes about disclosure, which are made clear within the document and to the students as service users.

# Complaints

Any person who is concerned about any aspect of the management of personal data can use the contact ASU and submit formal feedback via <https://www.astonsu.com/feedback/>

Any person who feels they are being denied access to personal information they are entitled to, or feels that their information has not been handled according to the Data Protection Principles, can contact the Information Commissioners Office at any time at ‘The Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.’ The Information Commissioner’s website is [www.ico.org.uk](http://www.ico.org.uk) and their telephone number is (+44) 1625 545700.

# Appendices

## Appendix A: Data Retention Schedule: Data Retention for Charities

|  |  |  |
| --- | --- | --- |
| **Record** | **Statutory retention period** | **Statutory authority** |
| accident books, accident records/reports | 3 years after the date of the last entry (see below for accidents involving chemicals or asbestos) | The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)  (SI 1995/3163) as amended |
| accounting records | 3 years for private companies, 6 years for public limited companies | Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006 |
| income tax and NI returns, income tax records and correspondence with the Inland Revenue | not less than 3 years after the end of the financial year to which they relate | The Income Tax (Employments) Regulations 1993  (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631) |
| medical records and details of biological tests under the Control of Lead at Work Regulations | 40 years from the date of the last entry | The Control of Lead at Work Regulations 1998  (SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676) |
| medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH) | 40 years from the date of the last entry | The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677) |
| medical records under the Control of Asbestos at Work Regulations  ·       medical records containing details of employees exposed to asbestos  ·       medical examination certificates | * 40 years from the date of the last entry * 4 years from the date of issue | The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/. 2739) |
| medical records under the Ionising Radiations Regulations 1999 | until the person reaches 75 years of age, but in any event for at least 50 years | The Ionising Radiations Regulations 1999  (SI 1999/3232) |
| records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH) | 5 years from the date on which the tests were carried out | The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677) |
| records relating to children | until the child reaches the age of 21 | Limitation Act 1980 |
| records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents | 6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed. | The Retirement Benefits Schemes (Information Powers) Regulations 1995  (SI 1995/3103) |
| Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence | 3 years after the end of the tax year in which the maternity period ends | The Statutory Maternity Pay (General) Regulations 1986  (SI 1986/1960) as amended |
| Statutory Sick Pay records, calculations, certificates, self-certificates | 3 years after the end of the tax year to which they relate | The Statutory Sick Pay (General) Regulations 1982  (SI 1982/894) as amended |
| wage/salary records (also overtime, bonuses, expenses) | 6 years | Taxes Management Act 1970 |

## Appendix B: Data Retention Schedule: HR/Finance/People related

### Recommended retention periods (i.e. where no statutory retention periods exist)

For many types of personnel records, there is no definitive retention period: it is up to the employer to decide how long to keep these records and it’s a question of judgment. An employer needs to consider what would be a necessary retention period, depending on the type of record. The advice in this factsheet is based on the time limits for potential tribunal or civil claims and aims to draw sensible conclusions as to how long keeping the records will protect an employer.

Where the recommended retention period given is 6 years, this is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980. Thus, where documents may be relevant to a contractual claim, it is recommended that these be retained for at least the corresponding 6-year limitation period.

|  |  |
| --- | --- |
| **Record** | **Recommended retention period** |
| actuarial valuation reports | permanently |
| application forms and interview notes (for unsuccessful candidates) | 6 months to a year. (Because of the time limits in the various discrimination Acts, for example the Disability Discrimination Act 1995, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. Successful job applicants’ documents will be transferred to the personnel file in any event.) |
| assessments under Health and Safety Regulations and records of consultations with safety representatives and committees | permanently |
| Inland Revenue approvals | permanently |
| money purchase details | 6 years after transfer or value taken |
| parental leave | 5 years from birth/adoption of the child or 18 years if the child receives a disability allowance |
| pension scheme investment policies | 12 years from the ending of any benefit payable under the policy |
| pensioners’ records | 12 years after benefit ceases |
| personnel files and training records (including disciplinary records and working time records) | 6 years after employment ceases |
| redundancy details, calculations of payments, refunds, notification to the Secretary of State | 6 years from the date of redundancy |
| senior executives’ records (that is, those on a senior management team or their equivalents) | permanently for historical purposes |
| time cards | 2 years after audit |
| trade union agreements | 10 years after ceasing to be effective |
| trust deeds and rules | permanently |
| trustees’ minutes | permanently |
| works council minutes | permanently |

## Appendix C: Data Retention Schedule: Data Retention for Aston Students’ Union Activity

|  |  |  |  |
| --- | --- | --- | --- |
| **Retention periods for Personal Data** | | | |
| **Type of data** | **Retention period** | **Reason for retention period** | **Action to be taken following retention period** |
| Membership information (e.g. Membership information, including society / sports / volunteers / course reps / | Until one year after student’s graduation | Service provision | Shred hard copy files, delete data files |
| Feedback and participation forms | During membership only | Benchmarking | Data can be kept in an anonymised format |
| Transport forms (e.g. driver registration forms) | During membership only | Service provision and audit | Shred hard copy files, delete data files |
| Positions of responsibility held within the Union | Indefinite | To keep accurate historical records of our engaged members | None. |
| Advice casework | Until seven years after a particular case has closed | Advice UK advice. Organisations can still be sued for negligence for up to 6 years after a case has closed | Shred hard copy files, delete data files |

## Appendix D: Guidelines for staff including Staff Checklist for Recording Data

Members of staff and officers will process personal data on a regular basis. The University and ASU will ensure that staff and students give their consent to processing.

Information about an individual's physical or mental health; sexual life; political or religious views; trade union membership; ethnicity or race; the commission of criminal offences and court proceedings dealing with criminal offences is sensitive and can normally only be collected and processed with their express consent.

Members of staff have a duty to make sure that they comply with the data protection principles, which are set out in the ASU Data Protection Policy. In particular, staff must ensure that records are:

* accurate;
* up-to-date;
* fair;
* kept and disposed of safely, and in accordance with ASU policy.

Individual members of staff are responsible for ensuring that all data they are holding is kept securely.

Members of staff must not disclose personal data, unless for normal democratic, membership or administrative purposes, without authorisation or agreement from the Data Protection Officer, or in line with ASU policy.

Before processing any personal data, all staff should consider the checklist.

All staff should complete online data protection training through Aston University (VLE).

**Staff Checklist for Recording Data**

* Do you really need to record the information?
* Is the information 'standard' or is it 'sensitive'?
* Have you conducted a Data Impact Assessment?
* If it is sensitive, do you have the data subject's express consent?
* Has the individual or data subject been told that this type of data will be processed?
* Are you authorised to collect/store/process the data?
* If yes, have you checked with the data subject that the data is accurate?
* Are you sure that the data is secure?
* If you do not have the data subject's consent to process, are you satisfied that one of the other conditions for processing data applies?
* How long do you need to keep the data for, and what is the mechanism for review/destruction?

## Appendix E: Data Protection Impact Assessment

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Department: | | | | |
| Lead Staff Member (Data Controller): | | | | |
| Data Processors: | | | | |
| Project Title: | | | | |
| Strategic Relevance: | | | | |
| What are the processing operations? | What are the legitimate interests? What is it being used for? | What risks are involved to individual data? | What measures are in place to mitigate those risks? | Further Notes / Observations |
|  |  |  |  |  |

1. http://advicequalitystandard.org.uk [↑](#footnote-ref-1)