LANCASTER UNIVERSITY STUDENTS' UNION

Lancaster University Students' Union Data Protection Policy

Approved by: Trustee Board
Implementation Date: May 2018
Review Date: May 2019
Policy Owner: Data Protection Officer

1. Introduction

1.1 In undertaking the business of Lancaster University Students' Union, we all create, gather, store and process large amounts of data on a variety of data subjects such as on student members (both current and former), staff, customers/suppliers and members of the public. Our use of personal data ranges from CCTV footage, financial transactions with commercial customers through to the processing a student members' details throughout their journey, to graduation and beyond.

1.2 Some of the data we create/collect and process will be other people's personal and/or sensitive data, i.e. data concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sexual life

1.3 As our recording and use of data continues to increase, it is more important than ever that every member of staff understands the law that exists in relation to data protection and staff responsibilities in ensuring that data is secured and protected in line with the law.

1.4 Data protection is an important part of the students' union's overall information security arrangements. All information must be handled safely and securely according to agreed policy. In addition to good practice, some data sets are subject to external legislation and it is vital that staff recognise both categories in their handling of information and data.

1.5 Data protection legislation has existed in the UK for many years with the Data Protection Act (1998). However, as of May 2018, new legislation has come into force - the General Data Protection Regulations (GDPR) and the Data Protection Bill 2018.

1.6 As the students' union processes 'personal data' of staff, student members and other individuals, it is defined as a Data Controller for the purposes of the GDPR. The students' union currently processes personal data strictly in accordance with Data Protection legislation and this will continue to be the case in relation to the GDPR.

1.7 The GDPR applies to all data relating to, and descriptive of, living individuals defined in the Regulations as 'personal data'. Individuals are referred to as 'data subjects'.

1.8 The GDPR places obligations on the students' union and the way it handles personal data. In turn the staff and members of the students' union have responsibilities to ensure personal data is processed fairly, lawfully and securely. This means that personal data should only be processed if we have a valid condition of processing (e.g. consent obtained from the data subject, legitimate interest or a contract with them) and we have provided information to the individuals concerned about how and why we are processing their information (i.e. a privacy notice). There are restrictions on what we are allowed to do with personal data such as passing personal information on to third parties, transferring information outside the EU or using it for direct marketing.

1.9 The Lancaster University Students' Union is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1.10 In the first instance an appointed Data Protection Officer will have responsibility for the Data Protection Policy. The Trustee Board has the authority to make revisions to the policy. The Union's Data Protection Officer will be responsible for bringing forward any revisions to the Board.

2. Statement of Policy

2.1 In order to operate both effectively and efficiently, Lancaster University Students' Union has to collect and use information about people with whom it works. These may include members of the union, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

2.2 This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act and GDPR to ensure this.

2.3 The union regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between itself and those with whom it carries out business.

2.4 The union will ensure that it treats personal information lawfully and correctly. To this end this policy sets out the responsibilities of the students' union, its staff and its student members to comply fully with the provisions of the GDPR. It is accompanied by a Data Protection Guidance Handbook with provides information and guidance on different aspects of data protection and data security. This policy, its associated policies and the Guidance Handbook form the framework from which staff and student members should operate to ensure compliance with data protection legislation.

3. Background

3.1 ***Data Protection Principles***

The students' union is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The six principles are:

3.1.1 Personal data shall be processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency').

3.1.2 Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any manner incompatible with those purposes. Further processing for archiving, scientific or historical research or statistical purposes is permissible ('purpose limitation')

3.1.3 Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed ('data minimisation').

3.1.4 Personal data shall be accurate and where necessary kept up to date ('accuracy').

3.1.5 Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose ('storage limitation').

3.1.6 Personal data shall be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

3.2 ***Personal Data***

3.2.1 Personal data is information about a living individual, who is identifiable from that information or who could be identified from that information when combined with other data which the students' union either holds or is likely to obtain. GDPR also refers separately to 'special categories' of personal data which includes particularly sensitive personal information such as health details, racial or ethnic origin or religious believes. Further information and guidance on personal data, including a full list of 'special categories' of personal data, is provided in section 2 of the Data Protection Guidance Handbook.

3.2.2 The definition of 'processing data' includes obtaining/collecting, recording, holding, storing, organising, adapting, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

3.2.3 The students' union, as data controller, remains responsible for the control of personal data it collects even if that data is later passed onto another organisation or is stored on systems or devices owned by other organisations or individuals (including devices personally owned by members of staff).

3.2.4 Staff developing new projects or processes or revising existing processes need to take data protection into account as part of this process and may need to carry out a data protection impact assessment.

3.2.5 In the event that there is a data protection breach this will usually have to be reported to the Information Commissioner's Office no later than 72 hours after the breach is discovered.

4. Implementation, Support and Guidance

4.1 All career staff, student staff, officers and volunteers within the Students' Union must be aware of the need to handle personal data in line with the Data Protection Bill 2018 and the General Data Protection Regulation. On commencement of employment or prior to gaining access to systems as a volunteer/officer an individual will be required to complete the training specified under Responsibilities & Training table in Appendix 6 of the Guidance Handbook.

4.1.1 This will be recorded within the union's relevant student or online training records.

4.1.2 The Data Protection Officer for Lancaster University Students' Union will be responsible for:

4.1.2.1 Implementing and monitoring the Data Protection Policy
4.1.2.2 Cascading the provision of training for staff, volunteers and student groups
4.1.2.3 Developing best practice guidelines
4.1.2.4 Carrying out compliance checks to ensure adherence with the relevant data protection regulations

4.2 The union management team will be responsible for making sure the policy is implemented across all departments of the union, under the guidance of the designated Data Protection Officer.

4.3 The Data Protection Officer **MUST** be informed of all data subject access requests received by staff or student groups within the union.

4.4 Advice on specific issues concerning the management and handling of personal data may also be contained within the relevant policy and are outlined in the Guidance Handbook.

5. Policy

The Policy is set out in the following sections:

5.1 General	5.9 Subject Access Requests and Data Subject Rights
5.2 Data Security	5.10 Data Sharing
5.3 Data Retention	5.11 Transfers of Personal Data Outside the EU
5.4 Conditions of Processing and Consent	5.12 Data Protection Impact Assessments & Data Protection by Design
5.5 Privacy Notices	5.13 Direct Marketing
5.6 Record of Processing Activities	5.14 Personal Data Breach
5.7 Children	5.15 Impact of Non-compliance
5.8 Research	

5.1 General

5.1.1 The students' union is responsible for demonstrating compliance with the six data protection principles

5.1.2 Compliance with the Data Protection Act 2018 and GDPR and adhering to these principles is the responsibility of all members of the students' union. Any deliberate breach of this policy may lead to disciplinary action being taken, access to students' union services and facilities being withdrawn, or even criminal prosecution.

5.1.3 The students' union is required to keep a record of its data processing activities as a summary of the processing and sharing of personal information and the retention and security measures that are in place. For more information about these records see 'Data Stored by the Union & Subsidiary Companies' in Appendix 7 of the guidance handbook.

5.2 Data Security

5.2.1 All students' union users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

5.2.2 Data Security should be undertaken in line with Students' Union and University procedures. Additional guidance on data security is included in section 4 of the Data Protection Guidance Handbook.

5.3 Data Retention

5.3.1 Individual areas within the students' union are responsible for ensuring the appropriate retention periods for the information they hold and manage, based on students' union guidance. Retention periods will be set based on legal and regulatory requirements, sector and good practice guidance. Retention periods are outlined in the

Data Stored by the Union & Subsidiary Companies in appendix 7 of the guidance handbook.

5.3.2 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. Once information is no longer needed is should be disposed of securely. Paper records should be shredded or disposed of in confidential waste and electronic records should be permanently deleted.

5.3.3 If data is fully anonymised then there are no time limits on storage from a data protection point of view.

5.4 Conditions of Processing and Consent

5.4.1 In order for it to be legal and appropriate for the students' union to process personal data at least one of the following conditions must be met:

5.4.1.1 The data subject has given his or her consent

5.4.1.2 The processing is required due to a contract

5.4.1.3 It is necessary due to a legal obligation

5.4.1.4 It is necessary to protect someone's vital interests (i.e. life or death situation)

5.4.1.5 It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. #

5.4.1.6 It is necessary for the legitimate interests of the controller or a third party and does not interfere with the rights and freedoms of the data subject (this condition cannot be used by public authorities in performance of their public tasks).

5.4.2 All processing of personal data carried out by the students' union must meet one or more of the conditions above. In addition the processing of 'special categories' of personal data requires extra, more stringent, conditions to be met in accordance with Article 9 of the GDPR.

5.4.3 The students' union shall maintain a central record of all the reasons for using personal data and the legal basis that we use for the processing of this. This shall be published as part of our privacy notice.

5.4.4 Consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or other clear affirmative action, signifies agreement to the processing of personal data relating to him or her". The GDPR clarifies that silence, pre-ticked boxes or inactivity does not constitute consent.

5.4.5 Anyone who has provided consent has the right to revoke their consent at any time.

5.4.6 Further information about obtaining consent can be found in section 5 of the Data Protection Guidance Handbook.

5.5 Privacy Notices

5.5.1 Under the 'fair and transparent' requirements of the first data protection principle, the students' union is required to provide data subjects with a 'privacy notice' to let them know what it does with their personal data (the main privacy notices for the students' union can be viewed at: https://lancastersu.co.uk/legal/privacy

5.5.2 Privacy notices are published on the students' union website and are therefore available to staff and student members from their first point of contact with the students' union. Any processing of staff or members data beyond the scope of the standard privacy notice, or processing of the personal information of any other individuals will mean that the existing privacy notice will have to be amended and members notified or a separate privacy notice will need to be provided.

5.5.3 Further information on what information should be included in a privacy notice is provided in section 5 of the Data Protection Guidance Handbook.

5.6 Records of Processing Activities

5.6.1 As a data controller the students' union is required to maintain a record of processing activities which covers all the processing of personal data carried out by the students' union. Amongst other things this record contains details of why the personal data is being processed, the types of individuals about which information is held, who the personal information is shared with and when personal information is transferred to countries outside the EU.

5.6.2 These records of processing activities shall be held centrally and maintained by the Data Protection Officer and can be accessed on request.

5.6.3 Staff embarking on new activities involving the use of personal data and that is not covered by one of the existing records of processing activities **MUST** inform the Data Protection Officer before starting the new activity as they may be required to undertake a Data Protection Privacy Impact Assessment.

5.7 Children

5.7.1 Under GDPR the following restrictions apply to the processing of personal information relating to children:

- Online services offered directly to children require parental consent.
- Any information provided to a child in relation to their rights as a data subject has to be concise, transparent, intelligible and easily accessible, using clear and plain language.
- The use of child data for marketing or for profiling requires specific protection.

5.7.2 The Data Protection Officer should be informed if any of the above activities are being contemplated.

5.8 Research

5.8.1 Data collected for the purposes of research are covered by the GDPR. It is important that staff collecting data for the purpose of research incorporate an appropriate form of consent on any data collection form.

5.8.2 Further information and guidance on data protection and research is provided in section 6 of the Data Protection Guidance Handbook.

5.9 Subject Access Requests and Data Subject Rights

5.9.1 The GDPR gives data subjects the right to access personal information held about them by the students' union. The purpose of a subject access request is to allow individuals to confirm the accuracy of personal data and check the lawfulness of processing to

allow them to exercise rights of correction or objection if necessary. However, individuals can request to see any information that the students' union holds about them which includes copies of email correspondence referring to them or opinions expressed about them.

5.9.2 The students' union must respond to all requests for personal information and information will normally be provided free of charge.

5.9.3 Data subjects are entitled to be told by Lancaster University Students' Union whether they are processing that individual's personal data, the purposes for which they are being processed, to whom they are or may be disclosed and to receive in an intelligible manner, a copy of their personal data.

5.9.4 Lancaster University Students' Union must ensure that it has proof of the identity of the requestor to prevent an unlawful disclosure.

5.9.5 A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.

5.9.6 Lancaster University Students' Union is required by the GDPR to respond within one month of receipt of the request, but every effort should be made to respond as quickly as possible. The one month applies to all requests for personal data, whether routine or complex but may be extended by up to two months if the complexity of a request makes this reasonable and the requestor is informed within an appropriate timeframe

5.9.7 The response should be provided in a commonly used electronic format, particularly if the request came in electronically, unless the requester asked for another format. When requested by the data subject the information may be provided orally as long as we are confident about the identity of the data subject.

5.9.8 If the request arises as part of another matter for instance a complaint, grievance or disciplinary matter, the requirements of the GDPR must not be overlooked, particularly the one month deadline. In these circumstances, staff must seek advice from the Data Protection Officer.

5.9.9 If an individual feels they are being denied access to personal information or have any other data protection grievances they can contact the Information Commissioners Office: https://ico.org.uk/concerns/.

5.9.10 For information about making a subject access request see the website https://lancastersu.co.uk/subject-access-request . Further information and guidance about handling subject access requests can be found in section 7 of the Data Protection Guidance Handbook.

5.9.11 Data subjects have a number of other rights under the GDPR. These include:

- **Right to Object –** Data subjects have the right to object to specific types of processing which includes processing for direct marketing, research or statistical purposes. The data subject needs to demonstrate grounds for objecting to the processing relating to their particular situation except in the case of direct marketing where it is an absolute right. Online services must offer an automated method of objecting.
- **Right to be forgotten (erasure) –** Individuals have the right to have their data erased in certain situations such as where the data are no longer required for the

purpose for which they were collected, the individual withdraws consent or the information is being processed unlawfully. There is an exemption to this for scientific or historical research purposes or statistical purposes if the erasure would render impossible or seriously impair the achievement of the objectives of the research. Individuals can ask the controller to 'restrict' processing of the data whilst complaints (for example, about accuracy) are resolved or the processing is unlawful.

- **Rights in relation to automated decision making and profiling** – The right relates to automated decisions or profiling that could result in significant affects to an individual. Profiling is the processing of data to evaluate, analyse or predict behaviour or any feature of their behaviour, preferences or identity. Individuals have the right not to be subject to decisions based solely on automated processing. When profiling is used, measures must be put in place to ensure security and reliability of services. Automated decision-taking based on sensitive data can only be done with explicit consent.
- **Right to Rectification -** The right to require a controller to rectify inaccuracies in personal data held about them. In some circumstances, if personal data are incomplete, an individual can require the controller to complete the data, or to record a supplementary statement.
- **Right to Portability –** the data subject has the right to request information about them is provided in a structured, commonly used and machine readable form so it can be sent to another data controller. This only applies to personal data that is processed by automated means (not paper records); to personal data which the data subject has provided to the controller, and only when it is being processed on the basis of consent or a contract.

5.9.12 Any requests made to invoke any of the rights above must be dealt with promptly and in any case within one month or receiving the request. Members of staff should consult the Data Protection Officer if any requests like these are received.

5.10 Data Sharing

5.10.1 Certain conditions need to be met before personal data can be shared with a third party or before an external data processor is used to process data on behalf of the students' union.

5.10.2 As a general rule personal data should not be passed on to third parties, particularly if it involves special categories of personal data but there are certain circumstances when it is permissible.

5.10.2.1 Any transfers of personal data must meet the data processing principles, in particular it must be lawful and fair to the data subjects concerned (see section 3.1)

5.10.2.2 It must meet one of the conditions of processing (see section 5.4). Legitimate reasons for transferring data would include:

- That is was a legal requirement
- It is **necessary** for the official core business of the students' union

5.10.2.3 If no other conditions are met then consent must be obtained from the individuals concerned and appropriate privacy notices provided (see section 5 on Consent & Privacy Notices in the Data Protection Guidance Handbook).

5.10.2.4 The students' union must be satisfied that the third party will meet all the requirements of GDPR particularly in terms of holding the information securely.

5.10.2.5 Where a third party is processing personal data on behalf of the students' union a written contract and/or a data sharing agreement **must** be in place. A contract is also advisable when data is being shared for reasons other than data processing so the students' union has assurances that GDPR requirements are being met.

5.10.3 Staff should consult with the Data Protection Officer if they are entering into a new contract that involves the sharing or processing of personal data.

5.10.4 Staff who receive requests for personal information from third parties such as relatives, police, local councils etc. should liaise with the Data Protection Officer. Section 9 of the Data Protection Guidance Handbook on Requests for Personal Information from Third Parties.

5.11 Transfers of Personal Data Outside the EU

5.11.1 Personal data can only be transferred out of the European Union under certain circumstances. The GDPR lists the factors that should be considered to ensure an adequate level of protection for the data and some exemptions under which the data can be exported. In many cases the students' union will require consent of the data subjects before personal information can be transferred out of the EU.

5.11.2 Information published on the internet must be considered to be an export of data outside the EU. This covers data stored in the cloud unless the service provider explicitly guarantees data storage only takes place within the EU. In the case of the students' union's main cloud storage on Box, binding corporate rules are in place which have been approved by the Information Commissioner as providing an adequate level of protection, however the same guarantees are not in place with other cloud providers.

5.11.3 The Information Commissioner's Office Guidance on the use of Cloud Computing should be consulted before any use of external computing resources or services via a network which may involve personal data.

5.12 Data Protection Impact Assessments and Data Protection by Design

5.12.1 Under the GDPR the students' union has an obligation to consider the impact on data privacy during all processing activities. This includes implementing appropriate technical and organisational measures to minimise the risk to personal data.

5.12.2 It is particularly important to consider privacy issues when considering new processing activities or setting up new procedures or systems that involve personal data. GDPR imposes a specific 'privacy by design' requirement emphasising the need to implement appropriate technical and organisational measures during the design stages of a process and throughout the lifecycle of the relevant data processing to ensure that privacy and protection of data is not an after-thought.

5.12.3 For some projects the GDPR requires that a Data Protection Impact Assessment (DPIA) is carried out. The types of circumstances when this is required include: those involving processing of large amounts of personal data, where there is automatic processing/profiling, processing of special categories of personal data, or monitoring of publicly assessable areas (i.e. CCTV). The DPIA is a mechanism for identifying and examining the impact of new initiatives and putting in place measures to minimise or reduce risks. Information about when and how to carry out a DPIA can be found in

section 11 of the Data Protection Guidance Handbook on Data Protection Impact Assessments.

5.13 Direct Marketing

5.13.1 Direct marketing relates to communication (regardless of media) with respect to advertising or marketing material that is directed to individuals e.g. all student emails etc. Individuals must be given the opportunity to remove themselves from lists or databases used for direct marketing purposes. The students' union must cease direct marketing activity if an individual requests the marketing to stop.

5.13.2 Direct marketing must also comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) which covers marketing via telephone, text and email.

5.14 Personal Data Breach

5.14.1 The students' union is responsible for ensuring appropriate and proportionate security for the personal data that we hold. This includes protecting the data against unauthorised or unlawful processing and against accidental loss, destruction or damage of the data. The students' union makes every effort to avoid personal data breaches, however, it is possible that mistakes will occur on occasions. Examples of personal data breaches include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Unauthorised disclosure (e.g. email sent to the incorrect recipient)
- Human error
- Hacking attack

5.14.2 If a data protection breach occurs the students' union is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

5.14.3 If you become aware of a data protection breach you must report it immediately. This should be done to the data protection officer, or in their absence a member of the senior management team. Details of how to report a breach and the information that will be required are included in section 14 of the Data Protection Guidance Handbook on Personal Data Breaches.

5.15 Impact of Non-compliance

5.15.1 All staff and student members of the students' union are required to comply with this Data Protection Policy, its supporting guidance and the requirements specified in the GDPR. Any member of staff or student who is found to have made an unauthorised disclosure of personal information or breached the terms of this Policy may be subject to disciplinary action. Staff may also incur criminal liability if they knowingly or recklessly obtain and/or disclose personal information without the consent of the students' union i.e. for their own purposes, which are outside the legitimate purposes of the students' union .

5.15.2 The students' union could be fined for non-compliance with the GDPR. There are two tiers of fines depending on the type of infringement.

6. Meeting our obligations

In order that our obligations are met the Union will ensure:

6.1 Organisation wide

6.1.1 That there is someone with specific responsibility for data protection in the organisation;

6.1.2 Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

6.1.3 Everyone managing and handling personal information is appropriately trained to do so;

6.1.4 Everyone managing and handling personal information is appropriately supervised;

6.1.5 Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

6.1.6 Queries about handling personal information are dealt with promptly and courteously;

6.1.7 Methods of handling personal information are regularly assessed and evaluated;

6.1.8 Performance with handling personal information is regularly assessed and evaluated;

6.1.9 Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

6.2 Staff & Officers of the Union

6.2.1 All elected officers are to be made fully aware of this policy and of their duties and responsibilities under the relevant data protection regulations.

6.2.2 All managers and staff within the Union will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised;
- All breaches of data protection will be reported to the Data Protection Officer as soon as possible;
- Computers/Devices are locked when not attended

6.3 3rd Parties

6.3.1 All contractors, consultants, partners or other agents of the Union must:

6.3.2 Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Union, are aware of this policy and are fully trained in

and are aware of their duties and responsibilities under the relevant data protection regulations.

6.3.3 Agree that any breach of any provision of the relevant data protection regulations will be deemed as being a breach of any contract between the Union and that individual, company, partner or firm;

6.3.4 Allow data protection audits by the Union of data held on its behalf (if requested);

6.3.5 Indemnify the Union against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.