Data Protection Policy

BY LAW of

CHESTER STUDENTS' UNION

Passed at Trustee Board on
23/04/2018

1. Introduction

1.1 Chester Students' Union ("CSU") is committed to complying with privacy and data protection laws including:

a. The General Data Protection Regulation ("the GDPR") and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017;
b. The Privacy and Electronic Communications Regulations (2203) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and
c. All other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO") or any other supervisory authority.

1.2 This policy sets out what we do to protect individual's personal data.

1.3 Anyone who handles personal data in any way on behalf of CSU must ensure that we comply with this policy. Section 3 of this policy describes what comes within the definition of personal data. Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

1.4 This policy may be amended from time to time to reflect the changes in legislation, regulatory guidance or internal policy decisions.

2. About this Policy

2.1 The types of personal data that we may handle include details of: students, employees, former employees, alumni and customers.

2.2 Gareth Pye is Chief Executive Officer of CSU and is responsible for ensuring compliance with the GDPR and with this policy. Any questions or concerns about this policy should be referred in the first instance to him via g.pye@chester.ac.uk or on 01244 511483.

3. Definitions of Data Protection Terms

3.1 The following terms will be used in this policy and are defined below:

3.2 Data Subjects include all living individuals about whom we hold personal data, for instance an employee or a supporter. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

3.3 Personal Data means any information relating to a living person who can be identified directly or indirectly from that information (or from that information 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). It can also include an identifier such as an identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

3.4 Data Controllers are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the legislation. CSU is the data controller of all personal data that we manage in connection with our work and activities.

3.5 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 other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

3.6 European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

3.7 ICO means the Information Commissioner's Office (the authority which oversees data protection in the UK).

3.8 Processing is any activity that involves the use of personal data, whether automated or not. It includes but is not limited to:

a) Collecting
b) Recording
c) Organising
d) Structuring
e) Storing
f) Adapting or altering
g) Retrieving
h) Disclosing by transmission
i) Disseminating or otherwise making available
j) Alignment or combination
k) Restricting
l) Erasing
m) Or destruction of personal data.

3.9 Sensitive Personal Data (which is defined as "special categories of personal data" under the GDPR) includes information about a person's:

a) Racial or ethnic origin
b) Political opinions
c) Religious, philosophical or similar beliefs
d) Trade union membership
e) Physical or mental health or condition
f) Sexual life or orientation
g) Genetic data
h) Biometric data and
i) Such other categories of personal data as may be designated as "special categories of personal data" under the legislation.

4. Data Protection Principles

4.1 Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any personal data that we deal with as a data controller.

4.2 Personal data should be:

a) Processed fairly, lawfully and transparently;
b) Collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes;
c) Adequate, relevant and limited to what is necessary for the purpose for which it is held;
d) Accurate and where necessary kept up to data;
e) Not kept longer than necessary; and
f) Processed in a manner that ensures appropriate security of the personal data.

5. Processing Data Fairly and Lawfully

5.1 The first data protection principle requires that personal data is obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions

can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons such as where it is necessary for the performance of a contract.

5.2 To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with "the fair processing information". In other words, we need to tell them:

a) The type of information we will be collecting (categories of personal data concerned);
b) Who will be holding their information ie. CSU including contact details of our Data Protection Officer;
c) Why we are collecting their information and what we intend to do with it for instance to process donations or send them a mailing about our activities;
d) The legal basis for collecting their information (for example are we relying on their consent, or on our legitimate interests or other legal basis);
e) If we are relying on legitimate business interests as a basis for processing, what those interests are;
f) Whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
g) The period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
h) Details of people or organisations with whom we will be sharing their personal data;
i) If relevant, the fact that we will be transferring their personal data outside the EEA and details of relevant safeguards; and
j) The existence of any automated decision-making including profiling in relation to that personal data.

5.3 Where we obtain personal data about a person from a source other than the person themselves, we must provide that individual with the following information in addition to that listed under 5.2 above:

a) The categories of personal data that we hold; and
b) The source of the personal data and whether this is a public source.

5.4 In addition, in both scenarios, (where personal data is obtained both directly and indirectly) we must inform individuals of their rights outlined in section 9 below, including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

5.5 This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

6. Processing Data for the Original Purpose

6.1 The second data protection principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

6.2 This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand.

7. Personal Data should be Adequate and Accurate

7.1 The third and fourth data protection principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of-date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

8. Not Retaining Data Longer than Necessary

8.1 The fifth data protection principle requires that we should not keep personal data for longer than we need to for the purposes it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. If you think that we are holding out of date data please speak to Gareth Pye.

8.2 For guidance on how long particular types of personal data that we collect should be kept before being destroyed or erased please contact Gareth Pye.

9. Rights of Individuals under the GDPR

9.1 The GDPR gives people rights in relation to how organisations process their personal data. Everyone who holds personal data on behalf of CSU needs to be aware of these rights. They include (but are not limited to) the right:

a) To request a copy of any personal data that we hold about them (as data controller), as well as a description of the type pf information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights)
b) To be told, where any information is not collected from the person directly, any available information as to the source of the information;
c) To be told of the existence of automated decision making;
d) To object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;
e) To have all personal data erased (the right to be forgotten) unless certain limited conditions apply;
f) To restrict processing where the individual has objected to the processing;
g) To have inaccurate data amended or destroyed; and
h) To prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

10. Data Security

10.1 The sixth data protection principle requires that we keep secure any personal data that we hold.

10.2 We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

10.3 When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

10.4 When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

10.5 The following security procedures and monitoring processes must be followed in relation to all personal data processed by us: backing up data (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up); staff should ensure that individual monitors do not show confidential information to passers-by and that they log off their PC when it is left unattended; paper documents should be shredded, memory sticks, CD Roms and other media on which personal data is stored should be physically destroyed when they are no longer required; personal data must always be transferred in a secure manner (the degree of security required will depend on the nature of the data – the more sensitive the data the more stringent the security measures should be); desks

and cupboards should be kept locked if they hold confidential information of any kind (personal data is always considered confidential) and staff must keep data secure when travelling or using it outside offices.

11. Transferring Data outside the EEA

11.1 The GDPR requires that when the organisation transfers personal data outside the EEA, they take steps to ensure that the data is properly protected.

11.2 The European commission has determined that certain countries provide an adequate data protection regime.

11.3 As such personal data may be transferred to people or organisations in these countries without the need to take additional steps beyond those you would take when sharing personal data with any other organisation. In transferring personal data to other countries outside the EEA (which are not on the approved list), it will be necessary to enter into an EC-Approved agreement, seek the explicit consent of the individual, or rely on one of the other derogations under the GDPR that apply to the transfer of personal data outside the EEA.

11.4 The EU-US Privacy Shield is an instrument that can be used as a legal basis for transferring personal data to organisations in the US, although specific advice should be sought from the data protection officer before transferring personal data to organisations in the US.

11.5 For more information, please speak to Gareth Pye.

12. Processing Sensitive Personal Data

12.1 On some occasions we may collect information about individuals that is defined by the GDPR as special categories of personal data and special rules will apply to the processing of this data.

12.2 Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data as the ICO will treat a breach to financial data very seriously.

12.3 In most cases, in order to process sensitive personal data, we must obtain explicit consent form the individuals concerned. As with any other types of information we will also have to be absolutely clear with people about how we are going to use their information.

12.4 It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please speak to Gareth Pye.

13. Monitoring and Review of the Policy

13.1 This policy is reviewed every three years by the Board of Trustees.