Data Protection Policy

Updated December 2020

1. Introduction

1.1. The Open University Students Association, "the Charity" is the Data Controller for the purposes of the Data Protection, Privacy and Electronic Communications Regulation 2019 (UK GDPR), The Data Protection Act 2018, The Privacy and Electronic Communications Regulation (PECR), the EU General Data Protection Regulation and any other data protection law that may be applicable.

1.2. The Charity collects and uses certain types of personal information about the following categories of individuals:

1.2.1. Staff (including OU staff);

1.2.2. Volunteers including External Trustees/Directors;

1.2.3. Members;

1.2.4. Honorary office holders and past office holders;

1.2.5. Alumni;

1.2.6. Societies, clubs and Group members;

1.2.7. And any other individuals who come into contact with the OU Students Association.

1.3. The Charity will process this personal information in the following ways:

1.3.1. To contact Open University students as members of the OU Students Association

1.3.2. To facilitate fair and proper elections for OU Students Association officer and representative positions via a secret ballot, in keeping with the duties under Section 22 of the Education Act 1994 (for this processing, the data is sent directly to the OU Students Association's nominated elections provider which is Civica Election Services (CES) Ltd via secure encrypted means. CES process the data to administer the elections on behalf of the OU Students Association).

1.3.3. To enable verification of individual student and study status

1.3.4. To facilitate and enable the processing of student complaints and moderation of shared online spaces, by either party

1.3.5. To enable student engagement in governance, to satisfy the aims of either/both party/parties.

1.3.6. To facilitate event management (e.g. Open University student consultation events, residential schools, OU Students Association biennial Conference etc)

1.3.7. To enable the celebration and proper storage of the history of the OU Students Association

1.3.8. To enable the work of the OU Students Shop to support the celebration and recognition of students' achievements in completing their studies and graduating from the institution

1.3.9. To facilitate research into the student experience and analysis of student feedback and engagement; for example, but not limited to, the National Students Survey, the OU Students Association Annual Membership survey and research projects;

1.3.10. To comply with statutory and contractual obligations relating to employment;

1.3.11. To comply with statutory and other legal obligations relating to safeguarding.

1.4. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the UK General Data Protection Regulation (the "GDPR") and other related legislation. It will apply to information regardless of the way it is used or recorded and applies for as long as the information is held.

1.5. The GDPR applies to all computerised data and manual files if they come within the definition of a filing system. Broadly speaking, a filing system is one where the data is structured in some way that it is searchable on the basis of specific criteria (so you would be able to use something like the individual's name to find their information), and if this is the case, it does not matter whether the information is located in a different physical location.

1.6. This policy will be updated as necessary to reflect best practice, or amendments made to the GDPR, and shall be reviewed every year.

2. Personal Data

2.1. 'Personal data' is information that identifies an individual and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain[1]. A sub-set of personal data is known as 'special category personal data'. This special category data is information that relates to:

2.1.1. race or ethnic origin;

2.1.2. political opinions;

2.1.3. religious or philosophical beliefs;

2.1.4. trade union membership;

2.1.5. physical or mental health;

[1] For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

2.1.6. an individual's sex life or sexual orientation;

2.1.7. genetic or biometric data for the purpose of uniquely identifying a natural person.

2.2. Special Category information is given special protection, and additional safeguards apply if this information is to be collected and used.

2.3. Information relating to criminal convictions shall only be held and processed where there is legal authority to do so.

3. The Data Protection Principles

3.1. The six data protection principles as laid down in the GDPR are followed at all times:

3.1.1. personal data shall be processed fairly, lawfully and in a transparent manner, and processing shall not be lawful unless one of the processing conditions can be met;

3.1.2. personal data shall be collected for specific, explicit, and legitimate purposes, and shall not be further processed in a manner incompatible with those purposes;

3.1.3. personal data shall be adequate, relevant, and limited to what is necessary for the purpose(s) for which it is being processed;

3.1.4. personal data shall be accurate and, where necessary, kept up to date;

3.1.5. personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes;

3.1.6. personal data shall be processed in such a way that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3.2. In addition to this, the Charity is committed to ensuring that at all times, anyone dealing with personal data shall be mindful of the individual's rights under the law (as explained in more detail in paragraphs 7 and 8 below).

3.3. The Charity is accountable to the principles in 3.1 which means that the Charity will:

3.3.1. when informing individuals as to the purpose and means of processing their information ensure a layered approach to its explanations, ensure information can be easily understood and ensure that links are provided to more expansive detail;

3.3.2. ensure the quality and accuracy of the information processed is periodically confirmed where this is possible. Those that can be identified are reminded that inaccuracies may be rectified ;

3.3.3. regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the Records Retention Policy;

3.3.4. ensure that when information is authorised for disposal it is done appropriately;

3.3.5. work with the Open University to ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system, and follow the relevant security policy requirements at all times;

3.3.6. share personal information with others only when it is necessary and legally appropriate to do so. Where necessary the charity will issue data sharing agreements and data processor agreements to protect the information ;

3.3.7. set out clear procedures for responding to requests for access to personal information known as subject access requests. The charity has developed procedures in accordance with the guidance of the Regulator;

3.3.8. report any breaches of the GDPR in accordance with the procedure in paragraph 9 below. The Charity has developed a procedure to identify when such breaches need to be reported to the Regulator.

3.3.9. take responsibility for complying with GDPR, which is implemented at the highest management level throughout our organisation and have measures in place that enable us to evidence our compliance. These include:

3.3.9.1. appointing a DPO;

3.3.9.2. working with our DPO to evaluate compliance and implement further measures where necessary;

3.3.9.3. regularly auditing the personal data collected, processed and stored and keeping a record of our processing activities;

3.3.9.4. carrying out Data Processing Impact Assessments (DPIAs) for all processing activities involving new technologies and/or where the processing of the data is likely to result in a high risk to individuals.

3.3.9.5. regularly reviewing and updating as necessary the technical and organisational measures we have in place to safeguard personal data.

4. Conditions for Processing in the First Data Protection Principle

Consent

4.1. Where the individual has given consent that is specific to the particular type of processing activity, and that consent is informed, unambiguous and freely given, we will additionally:

4.2. Ensure the request for consent is prominent and separate from other information and terms and conditions;

4.3. Provide separate opt ins for each data processing activity;

4.4. Be clear about the reason(s) for collecting the data, how it will be used and how long it will be kept;

4.5. Advise data subjects that they may opt out at any time and provide information about how to do this;

4.6. Keep consents obtained under review and refresh them if anything changes.

4.7. If special category or criminal offence data, as defined by the GDPR, is requested for the particular processing activity, the explicit consent of the data subject will be sought and recorded, separate to any other consents.

4.8. Our Appropriate Policy Document provides more detail on our processing or special category and criminal offence data.

Performance of a Contract

4.9. Where the charity enters into a contractual arrangement with an individual by providing a service or product in return for a consideration, personal data may be processed to uphold the performance of such an obligation or prior negotiations concerning such a contract.

4.10. The categories of data processed will only be those necessary to ensure the rights of the individual are upheld.

Legal Obligation

4.11. Where there is a legal obligation to which the charity is subject including but are not limited to employment law and disclosure of personal information for the prevention or detection of crime.

Vital Interests and Exemptions to Processing

4.12. Where the processing of data is regarded as necessary to protect an interest which is essential for the life of a data subject or another natural living individual. In some such settings, the charity may also provide for such processing by relying on exemptions detailed in the Data Protection Act 2018 Schedule 1, Part 2 sections 10, 16, 18 and 19 where there is a need to prevent or detect a crime, where support may be required for an individual with a particular disability or medical condition, where safeguarding may be needed for an individual at risk or where the economic wellbeing of an individual is at risk.

In the Public Interest

4.13. Where the charity is required to process data and is subject to an obligation in accordance with a specific law. The charity is obliged to use such a condition to ensure fair and democratic elections are conducted and may also apply this condition to other activities that support or promote democratic engagement, concern the biennial Conference or other charitable activities of the Association and where the Law permits.

In our Legitimate Interest

4.14. The charity will process personal data where required using this condition subject to the completion of a balancing test and where appropriate a Data Protection Impact Assessment (DPIA).

4.15. Such tests will measure the appropriateness of such processing by ensuring the interests of the charity do not outweigh the rights of data subjects as defined in the GDPR chapter III, Art.15(1)(a-h)(2)(3)(4), section 3, Art.16, 17, 18, 19 and 20. Section 4 Art.21 and 22, section 5 Art.23.

4.16. Evidence of such tests and assessments will be made available upon demand.

5. Disclosure of Personal Data

5.1. The following list includes the most usual reasons that the Charity will authorise disclosure of personal data to a third party:

5.1.1. to give a confidential reference relating to a current or former employee, or volunteer on receipt of the data subject's consent to do so;

5.1.2. for employment/HR reasons, e.g. to our payroll provider and pensions providers; or to our HR consultants for HR management reasons, in relation to the performance of the employment contract between the Charity and the data subject;

5.1.3. to enable fair and democratic elections, via exchange with the Open University and our elections provider Civica Election Services (CES), acting in accordance with the Charity's Articles of Association, in the public interest;

5.1.4. to facilitate event management, to include provision of data to hotels and venues to ensure student requirements and needs are met, on receipt of the data subject's consent to do so;

5.1.5. for the purpose of students and staff accessing campus and IT systems (being our legal obligation to manage access to support the prevention of crime and to comply with health and safety legislation);

5.1.6. for the prevention or detection of crime, in accordance with our legal obligation;

5.1.7. for the assessment of any tax or duty, in accordance with our legal obligation;

5.1.8. where it is necessary to exercise a right or obligation conferred or imposed by law upon us (other than an obligation imposed by contract);

5.1.9. for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);

5.1.10. for the purpose of obtaining legal advice, in accordance with our legitimate interests;

5.1.11. for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress), in our legitimate interests;

5.1.12. to fulfil our charitable objectives, we may provide data to third party services where stated in our Privacy Policy, which can be found on our website.

5.2. The Charity may receive requests from third parties (i.e. those other than the data subject, the Charity, and its employees) to disclose personal data it holds about individuals. This information will not generally be disclosed unless one of the specific exemptions under the GDPR which allow disclosure applies, or where disclosure is necessary for the legitimate interests of the third party concerned or the Charity.

5.3. All requests for the disclosure of personal data must be sent to the Chief Executive, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of the requesting third party before making any disclosure.

6. Security of Personal Data

6.1. The Charity will take reasonable steps to ensure that members of staff and volunteers will only have access to personal data where it is necessary for them to carry out their duties. All staff and volunteers will be made aware of this Policy and their duties under the GDPR. The Charity will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

6.2. For further details as regards security of IT systems, please refer to the ICT Policies of the Open University.

7. Subject Access Requests

7.1. Anybody who makes a request to see any personal information held about them by the Charity is making a subject access request. All information relating to the individual, including that held in electronic or manual files should be considered for disclosure, provided that they constitute a "filing system" (see clause 1.5).

7.2. Such requests may be answered according to the guidance of the Information Regulator which may include;

7.2.1. Providing transcripts of personal information as an adequate alternative to original documents;

7.2.2. Where such transcripts might not exist, the charity may not be able to provide such data;

7.2.3. Providing a predetermined selection of personal data as the charity sees appropriate;

7.2.4. Extending the time permitted to provide such information where the data subject is required to provide scope to such a search;

7.2.5. Not providing such data where the data may identify a third party, where there is a duty of confidentiality or where such data may reveal sensitive information about the charity's management forecasting or planning.

7.3. All requests should be sent to the Chief Executive within 3 working days of receipt and must be dealt with in full without delay and at the latest within one month of receipt (unless in exceptional circumstances).

7.4. Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Chief Executive must, however, be satisfied that:

7.4.1. the child or young person lacks sufficient understanding; and

7.4.2. the request made on behalf of the child or young person is in their interests.

7.5. Any individual, including a child or young person with ownership of their own information rights, may appoint another person to request access to their records. In such circumstances the Charity must have written evidence that the individual has authorised the person to make

the application and the Chief Executive must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

7.6. Access to records will be refused in instances where an exemption applies, for example, information sharing may place the individual at risk of significant harm or jeopardise police investigations into any alleged offence(s).

7.7. A subject access request must be made in writing. The Charity may ask for any further information reasonably required to locate the information.

7.8. An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where consent has not been given, or where seeking consent would not be reasonable, and it would not be appropriate to release the information. Particular care must be taken in the case of any complaint or dispute to ensure confidentiality is protected.

7.9. All files must be reviewed by the Chief Executive before any disclosure takes place. Access will not be granted before this review has taken place.

7.10. Where all the data in a document cannot be disclosed a permanent copy should be made and the data obscured or retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

Exemptions to Access by Data Subjects

7.11. The charity is committed to protecting information and strictly adheres to the exemptions which may include but are not limited to;

7.12. Where a claim to legal professional privilege could be maintained in legal proceedings, the information is likely to be exempt from disclosure unless the privilege is waived;

7.13. Where such data identifies a third party and the charity does not or cannot obtain the identified individual's consent;

7.14. Where the charity has a duty of confidentiality;

7.15. Where such data relates to the management of the charity including but not limited to matters concerning human resources and financial forecasting.

8. Other Rights of Individuals

8.1. The Charity has an obligation to comply with the rights of individuals under the law and takes these rights seriously. The following section sets out how the Charity will comply with the rights to:

8.1.1. object to processing;

8.1.2. rectification;

8.1.3. erasure; and

8.1.4. data portability.

Right to object to processing

8.2. An individual has the right to object to the processing of their personal data on the grounds of pursuit of a public interest or legitimate interest (grounds 4.6 and 4.7 above) where they do not believe that those grounds are made out.

8.3. Where such an objection is made, it must be sent to the Chief Executive within 2 working days of receipt, and they will assess whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals, or whether the information is required for the establishment, exercise or defence of legal proceedings.

8.4. The Chief Executive shall be responsible for notifying the individual of the outcome of their assessment within 20 working days of receipt of the objection.

8.5. Where personal data is being processed for direct marketing purposes an individual has the right to object at any time to processing of personal data concerning him or her for such marketing (which includes profiling to the extent that it is related to such direct marketing) and their personal data shall no longer be processed by the Charity for direct marketing purposes.

Right to rectification

8.6. An individual has the right to request the rectification of inaccurate data without undue delay. Where any request for rectification is received, it should be sent to the Chief Executive within 2 working days of receipt, and where adequate proof of inaccuracy is given, the data shall be amended as soon as reasonably practicable, and the individual notified.

8.7. Where there is a dispute as to the accuracy of the data, the request and reasons for refusal shall be noted alongside the data and communicated to the individual. The individual shall be given the option of a review under the complaint's procedure, or an appeal direct to the Information Commissioner.

8.8. An individual also has a right to have incomplete information completed by providing the missing data, and any information submitted in this way shall be updated without undue delay.

Right to erasure

8.9. Individuals have a right, in certain circumstances, to have data permanently erased without undue delay. This right arises in the following circumstances:

8.9.1. where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;

8.9.2. where consent is withdrawn and there is no other legal basis for the processing;

8.9.3. where an objection has been raised under the right to object, and found to be legitimate;

8.9.4. where personal data is being unlawfully processed (usually where one of the conditions for processing cannot be met);

8.9.5. where there is a legal obligation on the Charity to delete.

8.10. The Chief Executive will make a decision regarding any application for erasure of personal data and will balance the request against the exemptions provided for in the law. Where a decision is made to erase the data, and this data has been passed to other controllers, and/or has been made public, reasonable attempts to inform those controllers of the request shall be made.

Right to restrict processing

8.11. In the following circumstances, processing of an individual's personal data may be restricted:

8.11.1. where the accuracy of data has been contested, during the period when the Charity is attempting to verify the accuracy of the data;

8.11.2. where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;

8.11.3. where data would normally be deleted, but the individual has requested that their information be kept for the purpose of the establishment, exercise or defence of a legal claim;

8.11.4. where there has been an objection made under 8.2 above, pending the outcome of any decision.

Right to portability

8.12. If an individual wants to send their personal data to another organisation, they have a right to request that you provide their information in a structured, commonly used, and machine-readable format. If a request for this is made, it should be forwarded to the Chief Executive within 2 working days of receipt, and they will review and revert as necessary.

9. Breach of Any Requirement of the GDPR

9.1. Any and all breaches of the DPA, including a breach of any of the data protection principles shall be reported as soon as it is discovered, to the Data Protection Officer and to the Chief Executive

9.2. Once notified, they shall assess:

9.2.1. the extent of the breach;

9.2.2. the risks to the data subjects as a consequence of the breach;

9.2.3. any security measures in place that will protect the information;

9.2.4. any measures that can be taken immediately to mitigate the risk to the individuals.

9.3. Unless they conclude that there is unlikely to be any risk to individuals from the breach, it must be notified to the Information Commissioner's Office within 72 hours of the breach having come to the attention of the Charity, unless a delay can be justified.

9.4. The Information Commissioner shall be told:

9.4.1. details of the breach, including the volume of data at risk, and the number and categories of data subjects;

9.4.2. the contact point for any enquiries (which shall usually be the Data Protection Officer);

9.4.3. the likely consequences of the breach;

9.4.4. measures proposed or already taken to address the breach.

9.5. If the breach is likely to result in a high risk to the rights and freedoms of the affected individuals then the Chief Executive shall notify data subjects of the breach without undue delay unless the data would be unintelligible to those not authorised to access it, or measures have been taken to mitigate any risk to the affected individuals. The charity will determine the course of such action on a case by case basis.

9.6. Data subjects shall be told:

9.6.1. the nature of the breach;

9.6.2. who to contact with any questions;

9.6.3. measures taken to mitigate any risks.

9.7. The Chief Executive shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the Board of Trustees and a decision made about implementation of those recommendations.

10. International Transfers of Data and Article 27 Representation

10.1. Where data is stored by the Charity outside of the UK, necessary safeguards may be implemented to protect the fundamental rights and freedoms of those that may be identified by such data. Such safeguards may include the EU-US Privacy Shield for existing processing activities in light of the recent events (May 2020) to the validity of such arrangements. EU and UK Standard Contractual Clauses may also be implemented on a case-by-case basis.

10.2. Such safeguards may also be put in place where members of the Association reside outside of the UK. Where such members reside outside of the EU or the EEA Countries including Switzerland, an assessment of national laws may be considered on a case by case basis.

10.3. Where the data of individuals who reside in an EU state is processed in the UK, the Charity may appoint a representative in the EU to ensure the rights of those who are identifiable are upheld.

11. Contact

11.1. If anyone has any concerns or questions in relation to this policy, they should contact the Chief Executive in the first instance.