DATA PROTECTION AND INFORMATION SECURITY POLICY

Updated: February 2023

BUCKS STUDENTS' UNION

BUCKS STUDENTS' UNION POLICY DOCUMENT

Introduction

Bucks Students' Union ("we", "our" or "us") is committed to the protection of the personal data of our members, employees, suppliers and other individuals whom we might hold information about.

The Students' Union recognises the UK General Data Protection Regulation (UK GDPR) and the Privacy of Electronic Communications Regulations as the primary statutory responsibilities to data handling and processing.

To this end, every individual employee, student volunteer, member or contractor handling data collected or administered by the Union must take responsibility and due consideration for its appropriate use in line with this policy and the declared processing activities.

This policy applies to all employees and volunteers and is overseen by the Data Protection Officer reporting directly to the Strategy and Planning Committee, Finance and Staffing Committee and Trustee Board. Any deliberate breach of this policy may lead to disciplinary action being taken or even criminal prosecution. It may also result in personal liability for the individual.

Any questions or concerns about the interpretation or operation of this policy should be taken up with the Students' Unions Data Protection Officer.

Responsibilities

Students, suppliers and contractors

Students, suppliers and contractors must ensure that all personal data provided to the Union is accurate and up-to-date. They must ensure that changes of addresses or any other personal information is updated on the appropriate systems by contacting the relevant staff. Links to the respective privacy statements can be found online at bucksstudentsunion.org/privacy.

Student volunteers

Committee members, student reps and other student volunteers may handle personal data to administer their activities and services. When handling personal data, students are required to follow the guidance set out in the Data Protection and Information Security handbook which includes the reporting of data breaches, respecting the rights of individuals and secure processing procedures. Links to the handbook and privacy statements can be found online at bucksstudentsunion.org/privacy.

Union employees

The Students' Union holds various items of personal data about its employees, which are detailed in the relevant privacy statement and can be accessed through bucksstudentsunion.org/privacy. Employees must ensure that all personal data provided to the Union, in the process of employment, is accurate and up-to-date. They must ensure that changes of address etc are updated by contacting the HR and Development Manager.

In the course of day-to-day working, it is likely that staff will process individual personal data. Prior to handing any data, staff are required to have completed the University's Data Protection/Information Security Smart training course, through their eLearning platform. When handling personal data staff are required to follow the guidance set out in the Data Protection and Security Information handbook which can be accessed through bucksstudentsunion.org/privacy.

Union managers and project leads

Managers and project leads must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the framework agreed and identified within impact assessments, and are following the guidance set out in the Data Protection and Information Security handbook. For each point of data collection, a data impact assessment will be completed, outlining the legal basis for processing, what information is being collected and how it will be stored. These will be completed with department managers and reviewed on a regular basis with the Data Protection Officer in order to identify any weaknesses in information security.

Data Protection Officer

The Data Protection Officer is the Communications and Marketing Manager. They are responsible for:

- informing and advising the organisation and its employees about their obligations to comply with the UK GDPR and other relevant data protection laws
- monitoring compliance with the UK GDPR and other data protection laws, including managing internal data protection/processing activities, advise on data protection impact assessments, training of staff and conduct internal audits
- to be the first point of contact for supervisory authorities and for individuals whose data is processed.

The Data Protection Officer has delegated authority by the Board of Trustees and Chief Executive Officer to carry out their role with the resources required to be effective in the protection and security of the individual data the organisation handles.

The Data Protection Officer shall have full access to the email address sudataprotection@bucks.ac.uk.

Senior Management team

The Senior Management team is required to demonstrate ownership of the Union's Data Protection Policy and to communicate it across the organisation. Aspects of its management may be delegated to other levels of management.

Trustee Board

Trustee Board has overall accountability for the strategy of BSU and is responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Union. Trustee Board should seek assurance from the Senior Management team that effective arrangements are in place and are working through the Strategy and Planning Committee.

Compliance

Respecting individuals rights

The General Data Protection Regulations sets out a series of rights for individuals. BSU employees and volunteers planning data processing activities must record how these rights are addressed. The Data Protection and Information Security handbook details the rights and the organisation's standardised processes to meet these individual rights.

Processing special categories of data

BSU shall only process special categories of data linked to individuals, such as health data, religion and sexual orientation, with the consent of the individuals, except where the disclosure is to preserve life or for legal purposes. This data may also be analysed for statistical purposes where there is no direct link to an individual.

Subject access requests

The Data Protection and Information Security handbook details the procedures on how subject access requests should be handled. As standard, BSU does not charge any fee to comply with access requests and will refuse manifestly any unfounded or excessive requests. Any individual or department receiving a subject access request should send the completed paperwork to the Data Protection Officer straight away. The Data Protection Officer shall respond to the request within 30 days of receiving the necessary paperwork and proof of identity.

Lawful data processing

BSU shall only process data within the law. Where a lawful process has been identified, Union employees must inform the Data Protection Officer who will add it to the data source register. The Data Protection and Information Security handbook details the procedures on how to record the lawful processing justification.

Children

BSU staff and volunteers shall not process data relating to any individual under the age of 16.

Data breaches

BSU shall adopt processes to detect data breaches including audits and other appropriate processes. Employees shall report data breaches as outlined in the Data Protection and Information Security handbook.

Where an employee, volunteer, supplier or contractor discovers a data breach they must notify this to the Data Protection Officer within 24 hours. The Information Commissioner's Office shall be notified within 72 hours of the breach where there is a risk to the rights and freedoms of individuals, such as discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant disadvantage. Where there is a high risk to the rights and freedoms of individuals they shall also be directly notified. The reporting procedures are detailed in the Data Protection and Information Security handbook.

Data protection by design

Employees are required to adopt a 'privacy by design' approach to planning data collection and processing. In addition to data collection records, data impact assessments (DIAs) and, where appropriate, legitimate interest assessments (LIAs) shall be completed prior to any data collection or processing. DIAs and LIAs will be completed between the department manager and Union's Data Protection Officer.

Duty of confidence

Due to the nature of our work, and acting as a representative organisation for students, in certain circumstances, we are duty bound to protect the rights of other individuals, or other third parties, where information is disclosed to us confidentially. Where information is disclosed to us in express confidence, we have an obligation to respect this and we may treat this information as being exempt under the UK GDPR and Data Protection Act 2018. This will be treated on a case by case basis and we will endeavour to disclose as much information as possible, within the permitted boundaries of the law and respecting the duty of confidence to other individuals.

Information security

Data storage

Electronically stored personal data must be stored in an encrypted or password protected form to protect against unauthorised access or processing. Physical paperwork must be stored within a locked storage unit. When no longer needed, any digital copies should be permanently deleted and any physical paperwork securely destroyed. Staff should adhere to the retention periods that are outlined within the individual data impact assessments.

Vital records, for the purposes of business continuity, must be protected from loss, destruction or falsification by Union employees, in accordance with statutory, regulatory, contractual and Union policy requirements.

The Union has three primary platforms for securely storing electronic data: Buckinghamshire New University personal (G) drive, Buckinghamshire New University shared (S) drive and the main Union website. Staff are required to store data they handle on one of these platforms, as detailed within the Data Protection and Information Security handbook.

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from Union premises. Restricted information processed on portable devices and media must be encrypted. The password to an encrypted device must not be stored with the device and the password should be sufficiently strong.

Third-party contracts

Occasionally the Union may transfer data to third parties for processing in line with guidance contained within the Data Protection and Information Security handbook. Prior to data transfer, a contract to ensure compliance with relevant legislation must be in place with oversight from the Data Protection Officer.

IT systems

Employees must undertake the University's Data Protection/Information Security Smart training course, through their eLearning platform, to ensure sufficient awareness of data protection, GDPR and information security. Employees must make best attempts to protect their identity by using strong passwords for all platforms. Account password and usernames should not be shared.

Digital equipment and media containing information must be secured against theft, loss or unauthorised access when outside the Union's physical boundaries. In addition, all digital equipment and media must be disposed of securely and safely when no longer required.

Policy monitoring

Compliance with the policies and procedures laid down in this document will be monitored by the Union's Strategy and Planning Committee, together with reviews by the Finance and Staffing Committee and Trustee Board. The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a yearly basis unless there are significant changes to legislation.