Data Protection Policy

Board of Trustees Approval: 17/07/2017
Review Date: 17/07/2019

Introduction

The University of East London (UELSU) is committed to a policy of protecting the rights and privacy of individuals. UELSU needs to keep certain information on its Trustees, Employees, Elected Officers, Service Users, Volunteers and its members to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

We are committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person(s) unlawfully.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs. UELSU will remain the data controller for the information held. Volunteers will be personally responsible for processing and using personal information in accordance with the Data Protection Act.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with these data protection procedures. This document will also highlight the key data protection procedures within this organisation.

All staff, officers, volunteers and members who have access to personal information, will be expected to read and comply with this policy.

Purpose

The purpose of this policy is to set out the UELSU commitment and procedures for protecting personal data. UELSU regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

The Data Protection Act 1998

In line with the 8 principles as set out in the DPA UELSU will ensure that personal data will:

- Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
- Be obtained for a specific and lawful purpose
- Be adequate, relevant but not excessive
- Be accurate and kept up to date
- Not be held longer than necessary
- Be processed in accordance with the rights of data subjects
- Be subject to appropriate security measures
- Not to be transferred outside the European Economic Area (EEA)

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. UELSU will seek to abide by this code in relation to all the personal data it processes, i.e.

- Accountability: those handling personal data will follow publicised data principles to help gain public trust and safeguard personal data.

- Visibility: Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
- Consent: The collection and use of personal data must be fair and lawful and in accordance with the DPA's eight data protection principles. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject's consent should be explicitly obtained.
- Access: Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
- Stewardship: Those collecting personal data have a duty of care to protect this data throughout the data life span

Definitions

The following list are definitions of the terms used to aid understanding of this policy

Processing - is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes some paper based personal data as well as that kept on computer.

Data Controller – The person who (either alone or with others) decides what personal information UELSU will hold and how it will be held or used.

Data Protection Act 1998 (DPA) – The UK legislation that provides a framework for responsible behaviour of those using personal information

Data Protection Officer – The person of the Senior Manager Team (SMT) who is responsible for ensuring that UELSU follows its data protection policy and complies with the Data Protection Act 1998

Data Subject/Service User – The individual whose personal information is being held or processed by UELSU (for example: a service user or a volunteer)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject (see definition) to the processing of personal information about them.

Explicit consent is needed for processing sensitive data this includes the following:

(a) Racial or ethnic origin of the data subject

(b) Political opinions

(c) Religious beliefs or other beliefs of a similar nature

(d) Trade union membership

(e) Physical or mental health or condition

(f) Sexual orientation

(g) Criminal record

(h) Proceedings for any offence committed or alleged to have been committed

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Personal Information – Information about living individuals that enables them to be identified – e.g. names, addresses, telephone numbers and email addresses. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individual volunteers of the UELSU.

Notification –Notifying the Information Commissioners Office (ICO) about its data processing activities. The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is the Chief Executive Officer

Types of information processed

Examples of personal information on its employees, officers, volunteers, members and Trustees UELSU may process.

- Names
- Addresses
- Telephone numbers
- Email addresses

Sensitive data – refers to data about:

- Racial or ethnic origin
- Political affiliations
- Religion or similar beliefs
- Trade union membership
- Physical or mental health
- Sexuality
- Criminal record or proceedings
- Information on applicants for posts, including references
- Employee information –bank account number, payroll information, supervision and appraisal notes.
- Case notes on users of UELSU Student Support Service

Personal information is kept in both paper based and electronic formats.

Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of UELSU, this is the University of East London Students' Union Trustee Board.

The CEO/Trustee Board? is the Data Controller under the DPA and is legally responsible for complying with the DPA, which means that it determines what purposes personal information held will be used for.

The SMT will take into account legal requirements and ensure that it is properly implemented and through appropriate management apply strict criteria and controls.

Groups of people within the organisation who will process personal information are: employed staff, trustees and other volunteers- only those who will have process personal information

It is the responsibility of the **Data Controller** to:

- Observe fully conditions regarding the fair collection and use of information,
- Ensure UELSU meet its legal obligations to specify the purposes for which information is used.
- Ensure that UELSU collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the Act. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information

It is the responsibility of the **Data Protection Officer** to:

- Ensure that everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Ensure that everyone processing personal information is appropriately trained to do so
- Ensure that everyone processing personal information is appropriately supervised
- Make all aware that anybody wanting to make enquiries about handling personal information knows what to do
- Deal promptly and courteously with any enquiries about handling personal information
- Describe clearly how UELSU handles personal information
- To regularly review and audit the ways UELSU hold, manage and use personal information
- To regularly assess and evaluate its methods and performance in relation to handling personal information

It is the responsibility of all groups of people who process personal data to:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

Breaches of the rules and procedures identified in this policy may lead to disciplinary action being taken.

Board of Trustees Approval: 17/07/2017
Review Date: 17/07/2019

Training & Awareness

Raising awareness about the DPA and how it is followed may take the following forms:

On Induction - As part of the induction process new employees are given a copy of this policy and informed on how UELSU collects and uses data about them. (Induction Booklet)

As part of procedures for collecting membership data (Societies Training, Advice Service)

As part of a project planning process should data collection be an element

Annual reminders in team meetings (SMT, Leadership and general staff meetings)

Annual evaluation of the policy and its effectiveness

Biannually when the policy is due to reviewed.

Gathering and Information Collecting

Before any personal information is collected we will consider the following:

- The purpose/need for the information – e.g. to collect membership data for the purpose of voting in a UELSU Election
- The length of time the information needs to be held
- The content of the information gathered – will it be non-identifying data, personal information and or sensitive data?
- Where and how will the information be stored? – On UELSU hosted website or by the University of East London. Paper based or electronic

We will inform those whose information is gathered about the following:

- UELSU Data Protection Policy
- Privacy Policy (for website users)

We will take these measures to ensure that personal information kept is accurate:

- Employee information annually through annual performance review process, one on one meetings and through requests.
- Membership information – Through updates received from UEL about student status and therefore eligibility of membership to UELSU.
- Action requests received from Data Subject/Service User

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

Data Security

UELSU will take steps to ensure that personal data is secure at all time against unauthorised or unlawful loss or disclosure. The following measure will be taken:

- Information and records relating to service users will be stored securely and will only be accessible to authorised staff and volunteers.
- Information will be stored for only as long as it is needed or required statute and will be disposed of appropriately.

- UESU will ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.
- Using lockable cupboards (restricted access to keys)
- Password protection on personal information files
- Setting up computer systems to allow restricted access to certain areas
- Not allowing personal data to be taken off site in the forms of paper or memory stick
- If personal data is taken off site, the only form allowed is a laptop with password protected access
- Access to online personal data only accessible to authorised staff and volunteers
- Password protected attachments for sensitive personal information sent by email

Any unauthorised discourse of personal data to a third party by a staff member, may result in disciplinary action been taken against them.

Any unauthorised discourse of personal data to a third party by a volunteer, may result in disciplinary action been taken against them and or a termination of their services to UELSU or any volunteering agreement.

The Trustee Board are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach they may have made.

Subject Access Requests

Anyone whose personal information we process has the right to know:

- What information we hold and process on them
- How to gain access to this information
- How to keep it up to date
- What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer and certain files. Any person wishing to exercise this right should apply in writing to:

Chief Executive Officer
University of East London Students' Union
UEL Docklands Campus North Building
4 – 6 University Way
London E16 2RD

UELSU may make a charge of £10 on each occasion access is requested.

The following information will be required before access is granted:

- Full name and contact details of the person making the request
- The person's relationship with UELSU (former/ current member of staff, trustee or other volunteer, service user)
- Timescales Involved such as dates when the information was taken, dates of when the person left the employment of UELSU etc.

We may also require proof of identity before access is granted. The following forms of ID will be required:

- Passport
- Birth Certificate
- A current and valid driver's licence
- A current and valid National/Citizen ID Card
- A current and valid form of a government recognised Age Identity Card

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 40 days required by the Act from receiving the written request (and relevant fee).

Review

This policy will be reviewed at intervals of every 2 years to ensure it remains up to date and compliant with the law.

Board of Trustees Approval: 17/07/2017
Review Date: 17/07/2019