Data Protection Policy

© The University of Law 2016

CONTENTS

CLAUSE

© The University of Law 2016

1.0 Purpose and Scope

The purpose of the Data Protection Procedures and Standards are to ensure the Employees' roles and responsibilities with respect to protecting personal data are clearly defined, understood and followed by all Employees. The document also demonstrates how The University of Law implements the Data Protection Policy and Standards.

The procedure is applicable to all areas of The University of Law and sets out the requirements, standards and expectations for the protection of Personal Data relating to an identifiable Data Subject.

2.1 Definitions

- Contractors – This includes individuals who are independent contractors or contingent workers.
- Data Protection Officer (DPO) – The Data Protection Officer is responsible for the oversight, development and maintenance of all data protection /privacy functions within The University of Law. The DPO ensures compliance with all applicable laws and regulations and with this procedure and standards.
- Data Protection/Privacy Event – Any situation, whether suspected or proven, deliberate or inadvertent, that exposes the Personal Data of a Data Subject to unauthorised individuals.
- Data – Information that is either processed by or intended to be processed by, in response to instructions given for that purpose; or information that is recorded as part of, or with the intention of forming part of, a "relevant filing system" of information that forms part of an accessible record (as defined by the Data Protection Action 2018 or the General Data Protection Regulation).
- Data Controller – A person or organisation that makes decisions in regard to the Personal Data to be processed. The Data Controller decides the purpose for which Personal Data is to be processed, what Personal Data is required and how it is obtained.
- Data Processor - A Data Processor is any person (other than an employee of the Data Controller) that processes Personal Data on behalf of the Data Controller.
- Data Subject – A living individual. Data Subject include, but are not limited to, Students, Employees, Contractors, Tutors and Examiners.
- Employees – Current and former employees of The University of Law.
- Personal Data – Recorded information that relates to a living person that can be associated with that person, either from other information in the possession of the organisation holding the data or by cross referencing to information held by a third party. This includes expressions of option about the individual and indication of any intentions of the Data Controller or any other person in regard to the individual. Recorded information can be stored electronically or in a manual filing system.

Examples of Personal Data include

- Name, home and work addresses
- Date of Birth
- National insurance and passport numbers
- Bank account or credit card details
- Insurance policy details
- Employment records held by the employer
- Images caught on close circuit television (CCTV)
- Student record information
- Student exam results

Processing- in relation to information or data means obtaining, recording or holding the information or data and any operation performed on the information or data such as viewing, amending, sharing, deleting, or storing or any other use that might be done to or with the data.

Sensitive Personal Data – Personal Data of the Data Subject consisting of information as to their racial or ethnic origins, political opinions, religious beliefs, trade union membership, physical and mental health (including disabilities), sexual life, the commission or alleged commission of any offence and any legal proceedings (including the disposal of legal proceedings) or any court sentence in connection with any offence committed or alleged to have been committed by the Data Subject.

Data Subject Access Requests – Data Subject rights to information about the Personal Data relating to them which is in the control of the Data Controller.

3.1 Roles and Responsibilities

All Employees , students and contractors of The University of Law managing and handling Personal Data need to understand their responsibility for good data protection practice and must follow the procedures outlined below.

- Be aware of this policy and comply with it.
- Understand which information they have the right of access to.
- Know the information for which they are owners.
- Know the information systems and computer hardware for which they are responsible.

4.0 Governance

Responsibility for the production, maintenance and communication of this policy document and any sub-policy documents lies with the University's Data Protection Officer.
Each of the documents constituting the Data Protection Procedures and Standards will be reviewed annually. It is the responsibility of the DPO to ensure that these reviews take place.
Any substantive changes made to any of the documents in the set will be communicated to all relevant personnel.

5.1 University of Law (Ulaw) Employees

When a new Employee joins The University of Law they must undertake the induction training which will include data protection training. This training must be completed within the required timeframe.

All University of Law current employees will receive ongoing data protection training where required.

Participation will be tracked and reported to the DPO.

All employees are required to:

- Adhere to these procedures and standards, any further guidelines issued and the overarching DP/Privacy Policy.
- Complete the online training.

6.0 Managers

Managers must ensure that everyone managing and handling Personal Data is appropriately trained to do so and that everyone managing and handling Personal Data is appropriately supervised.

At the local level, the manager is responsible for ensuring that:

These procedures and standards and any further guidelines are followed.

These procedures and standards are fully implemented within their department.

7.1 Overall Organisations responsibilities – Data Protection Officer (DPO)

The role of the DPO is to

- Oversee University of Law compliance with the Data Protection Act 2018 and General Data Protection Regulation (GDPR), other applicable statutory laws, ICO regulations and guidance and the DP / Privacy Policy.
- Ensure that these procedures and standards regarding the processing of Personal Data are compliant with the Data Protection Act 2018,GDPR and other applicable statutory laws, ICO Regulations and guidance and the DP / Privacy Policy, and Implemented.
- Oversee responses to subject access requests across departments in addition to The University of Law nominated officer.
- Ensure relevant data protection / privacy notices are used and relevant consents are obtained
- Keep the relevant registrations up to date with the ICO.
- Investigate and track any Breaches in Data Protection Law and report to the members of the Executive Team and GUS Group Privacy Officer where necessary.
- Promote training and awareness.
- Oversee regular monitoring of Data Protection issues.
- Conduct ad hoc reviews where required.
- Provide guidance and answer any Data Protection queries from the business where required.
- Ensure Data Protection Impact Assessments (DPIA) or other appropriate assessments are carried out where required.

Should there be any issues that cannot be resolved locally the DPO should be contacted. The use of these procedures and standards and any further guidelines may be audited from time to time by the DPO.

8.1 Processing Personal Data fairly and lawfully.

The University of Law holds Personal Data about a Data Subject that is sufficient for the purpose it is being held in relation to that Data Subject, and The University of Law does not hold more information than needed for that purpose. The minimum amount of Personal Data needed to fulfil the purpose for processing should be identified. Only this information should be held and no more. This is part of the practice known as "data minimisation".Personal Data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Internal data sharing requests between departs should be reviewed by the DPO for reasonableness when

there is no operating agreement already in existence with the focus being on limiting the amount of Student/Customer and Employee Personal Data shared.

Employees/business owners/project managers must ensure any new projects and/or transmissions of data outside the Business Unit or organisation are referred to the DPO, when there is no operating agreement already in existence. When sharing or transmitting data outside the Business Unit or organisation the least amount of Personal Data necessary to fulfil the operational need should be transmitted. The DPO must assess the risk by completing a DPIA (Data Privacy Impact Assessment) and approve the Personal Data items.

8.2 Privacy Notices

Privacy Notices must adequately describe

- The University of Law as the Data Controller.
- Why the Personal Data is collected and how The University of Law intends to use the Personal Data collected about the Data Subject.
- If The University of Law intends to share the Personal Data and who it will be shared with.
- The types of information collected constituting Personal Data and the methods of collection.
- All privacy notices must be reviewed and approved by the DPO and The University of Law Legal Team.

Privacy notices are updated when there are updates to these procedures and standards or operational practice.

8.3 Personal Data must be processed fairly and lawfully. In practice, it means the following:

- Legitimate grounds must exist for collecting and using the Personal Data. Particular care has to be given in relation to the processing of Sensitive Personal Data; in general Sensitive Personal Data can only be processed with the explicit consent of the Data Subject and must be kept secure at all times.

In instances where it is suspected that a data subject may be suffering from a mental health condition, or be classed as vulnerable, by way of age, disability or otherwise advice should be sought from the DPO, or the mental health subject matter experts.

8.4 Personal Data should not be used in ways that have unjustified adverse effects on the Data Subjects concerned.

- Data Subjects should be provided with appropriate privacy notices when their personal data is being collected to ensure transparency about the intended use of their Personal Data.
- Personal Data should only be handled in ways they would reasonably expect
- The personal data should not be used in any unlawful way or for any unlawful purpose

New or changed methods of collecting Personal Data must be reviewed by the DPO before they are implemented to confirm that Personal Data is obtained fairly and lawfully. This may be done by utilising the DPIA (Data Privacy Impact Assessment form) which is available from the Data Protection Officer.

8.5 Processing Personal Data

The University of Law must ensure that the Information Commissioner's Office (ICO) is kept informed of all the current uses of Personal Data. This is achieved by a notification given to the Information Commissioner.

If any process is removed this must also be communicated to the DPO.

The DPO is responsible for ensuring that the University of Law's ICO registration remains accurate and up to date. There is an obligation to inform the ICO of any changes to the registration within 28 days from when the change occurred. The University of Law's registration is required to be renewed annually.

Personal Data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

This requirement aims to ensure that organisations are open about their reasons for obtaining Personal Data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

8.6 Keeping Personal Data accurate and up to date

Take reasonable steps to ensure the accuracy of any Personal Data obtained and ensure that the source of any Personal Data is clear, carefully consider any challenges to the accuracy of information and consider whether it is necessary to update the information.

The University of Law informs Data Subjects that they have the right to amend or delete incorrect data in the privacy notices provided to Employees and customers. The University of Law also contractually obliges Data Subjects who are our students/customers to notify us of any changes in their details. The University of Law performs data quality reviews on an ad hoc basis or when required to ensure that the data managed or processed is accurate and up to date. This includes reviews, data integrity controls and process review.

8.7 Retaining Personal Data

Review the length of time the Personal Data is kept; Consider the purpose or purposes for holding the information when deciding whether (and for how long) to retain it; Securely delete information that is no longer needed for this purpose or these purposes and update, archive or securely delete information if it becomes out of date.

Personal Data must be destroyed according to guidelines specified within the University of Law retention Policy.

9.1 The Rights of the Data Subject.

Personal Data shall be processed in accordance with the rights of Data Subjects under the DPA. The rights of the Data Subject are:

Right of access – Data subjects have a right to access to your data and to certain information about the processing of that personal data. This information must usually be provided to you free of charge within a month of receiving your request. Exceptions to this are:

- Examination scripts which are specifically exempt from the data subject's access rights under the General Data Protection Regulation. In general, students are entitled to know their examination marks but are not entitled to see their examination scripts. However, students are entitled to see associated examiner's comments and minutes of any examination appeals panels, which are not exempt from disclosure.
- Examination marks that have been requested before the results are announced have to be

disclosed either within 5 months of the date of the request or within 30 days of the date the results are published, whichever is earlier. In practice, this exemption prevents disclosure of exam results before they are officially announced

Right of rectification (correction) – you have the right to ask for your personal data to be corrected if it is inaccurate and completed if it is incomplete.

Rights to be forgotten- in certain circumstances you can ask us to erase your personal data. It is unlikely to be possible to accept your request if, for example, we have a contractual or other legal duty to retain your information.

Right to restriction of processing – in certain circumstances you have a right to restrict the processing of your personal data. This may include when you dispute its accuracy (until the accuracy is proved); if you have objected to the processing (when it was necessary for our legitimate interest) and we are considering whether our legitimate interest overrides your own; or if we no longer need the data but you need us to keep it in order to establish, exercise or defend a legal claim.

Right of portability – in certain circumstances, you have the right to move, copy or transfer your data to another data controller or to yourself. This right is only relevant if the data is being processed on the basis of consent or for the performance of a contract and the processing is carried out by automated means. This right is different from the right of access and the types of information you can get under the two separate rights may be different.

Rights in relation to automated decision making – you may have the right to challenge and request a review of a decision that was made by automated means.

Right to object – in certain circumstances, you have the right to object to the processing of your data when it is being processed on the basis of our legitimate interest. We must stop processing the data unless we can demonstrate that our legitimate interests override your own, or if the processing is necessary for legal reasons. You have an absolute right to object to processing your data for direct marketing purposes including profiling relevant to direct marketing. If you object to us processing your data for direct marketing purposes, we must accept your request and stop the processing as soon as we receive your objection.

Additional detailed information on Data Rights can be found in the Data Protection Rights Policy

9.2 Right of Access to Personal Data

The Data Protection Act 2018 gives Data Subjects the right to access the personal information that is processed about them. This right is commonly referred to as subject access. Some types of Personal Data are exempt from the right of subject access and so cannot be obtained by making a Data Subject Access Request (DSAR). If there is any doubt in the types of data that can be supplied under a DSAR, the matter should be referred to the DPO for clarity.

Under this right the Data Subjects is entitled to:

- Be informed by any Data Controller whether Personal Data which relates to the individual is being processed by or on behalf of that Data Controller.
- Be given a description of the information constituting Personal Data of which the individual is the Data Subject. Be given a description of the purposes for which their Personal Data is being or is to be processed.
- Be given a description of the recipients or classes of recipients to whom their Personal Data is being or may be disclosed.
- Be provided a copy of the information constituting any Personal Data of which the individual is the Data Subject in a form that is capable of being understood.

- Be provided details of any information available to the Data Controller as to the source of the Personal Data (where available) in a form that is capable of being understood.

- Be provided (if specifically requested by the Data Subject) with the logic involved where the processing by automatic means of Personal Data of the Data Subject for the purpose of evaluating matters relating to the Data Subject e.g. performance at work, creditworthiness, has constituted or is likely to constitute the sole basis for any decision significantly affecting the Data Subject

A Data Subject must make a DSAR in writing to the Data Controller, a request sent by email or fax is acceptable. However, it cannot be insisted upon that a DSAR is made in a particular format. If the DSAR does not refer to the Data Protection Act specifically or state that it is a DSAR it should still be treated as valid, if it is clear that the Data Subject is asking for their own Personal Data, There is no charge to provide the Personal Data requested.

If there is uncertainty as to the identity of a Data Subject making the DSAR, additional information should be requested from the Data Subject to verify their identity. This should be an official document - e.g. a council tax bill, driving licence or passport.

A Data Subject is entitled to make a DSAR via a third party. In this case the Data Controller needs to be satisfied that the third party making the request is entitled to act on behalf of the Data Subject. If you believe an individual may not understand what information would be disclosed to a third party who has made a DSAR on their behalf, you may send the response directly to the individual rather than the third party. The individual will then have the chance to review the data before deciding whether to share it with the third party.

In some cases an individual will not have the mental capacity to manage their own affairs. However, it is reasonable to assume that an attorney with the authority to manage the individual's affairs, or appointed by the Court of Protection to make decisions about such matters, will have the appropriate authority. Any concerns should be raised with the DPO.

Further clarity regarding the information requested in the DSAR can be requested from the Data Subject. For example, if a Data Subject has requested Personal Data contained in emails, you may ask for the dates the emails were sent.

If the response to a DSAR involves providing information that relates to the Data Subject and another individual who can be identified from that information, either the consent of the individual is required or it must be reasonable in all circumstances to comply with the request without the individual's consent. Any concerns should be raised with the DPO.

9.1.1 Responding to a DSAR

A DSAR must be responded to no later than 30 days after it has been received by the Data Controller.

The 30-day period does not start until: The University of Law as the Data Controller is satisfied as to the identity of the Data Subject making the DSAR; and the additional information reasonably needed to find the Personal Data has been supplied by the Data Subject.

However, it is not acceptable to delay responding to a DSAR unless more information is reasonably required to locate the Personal Data in question. The Data Subject has a right to see the information contained in the Personal Data rather than a right to see the documents that include that information. The information requested must be provided in a permanent format - such as a computer printout, letter or form - unless: The Data Subject agrees otherwise: It is not possible to supply such a copy: or It will involve undue effort; this includes very significant cost or effort to produce the information in hard copy. If this is the case, you must still provide access to the information in another way. You must also ensure that the information can be understood, for example, if there are any codes used, you should explain what they mean.

All subject access requests are dealt with by the DPO. If you receive a DSAR you must pass it to the DPO immediately.

9.2 Right to preventing processing likely to cause damage or distress

A Data Subject has a right to object to processing only if it causes unwarranted and substantial damage or distress. If it does, they have the right to require an organisation to stop (or not to begin) the processing in question. In such circumstances the Data Subject may be able to require a Data Controller to not begin or to stop processing their personal Data. This right is limited to certain circumstances; if such circumstances do not apply the Data Controller has to provide an explanation to the Data Subject as to why it has no requirement to comply with the objection to processing.

There are a number of points to consider when deciding whether and to what extent there is an intention to comply with an objection to processing, such as, is the objection to processing in writing. An objection has to be in writing (which includes an email or fax). Once received, there is a time limit of 21 calendar days in which to provide a response to the Data Subject. The response must state what is intended to be done or if there is no intention to comply with the objection to processing and an explanation of why there is no requirement for the Data Controller to comply with the objection to processing.

Does the objection explain how the processing is/will cause unwarranted and substantial damage or distress. If it is not clear in the objection as to the extent of the problem the processing would be/is causing, the Data Subject may need to provide further clarification in order for a decision as to whether to comply with the objection to processing to be made or whether there is no requirement on the Data Controller to do so. A response (as set out above) must be provided to the Data Subject.

9.2.1 Processing that can be relied on to Legitimise the Processing.

- The Data Subject has given their consent to the processing.
- The processing is necessary for the performance of a contract to which the data subject is a party or for the taking of steps at the request of the data subject with a view to entering into a contract.
- The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.
- The processing is necessary in order to protect the vital interests of the data subject.

All objections to data processing are dealt with by the DPO. If you receive an objection from a data subject you must pass it to the DPO immediately.

9.3 The Right to Prevent Direct Marketing

Data Subjects have the right to prevent their personal Data being processed for direct marketing.

A Data Subject can at any time give written notice to The University of Law as the Data Controller to stop (or not begin) using their Personal Data for direct marketing. Any Data Subject can exercise this right, and if such a notice is received it must be complied with in a reasonable period. Direct marketing can take many forms and therefore the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) provide rules about sending marketing and advertising by electronic means, such as by phone, fax, email, text and picture or video message or by using an automated calling system. PECR also include other rules relating to cookies, telephone directories, traffic data and security breaches.

Data Subjects have the right to opt out of receiving marketing at any time. The Data Controller should not send marketing texts or emails to a Data Subject who has said they do not wish to receive them. Data Controllers must comply with any written objections promptly to comply with the Data Protection Act 2018, but even if there is no written objection, as soon as an individual says they do not want emails or texts, this will override any existing consent or soft opt in under PECR and they must stop.

Data Controllers should not make it difficult to opt-out of marking communications. If any Data Subject objects or opts out at any time, their details should be suppressed from any marketing lists as soon as possible.

If you receive a request from a Data Subject to be removed from the marketing list you must pass this to the relevant Marketing team immediately.

9.4 Rights in relation to decisions taken by Automated Means

A Data Subject can send a written notice to a Data Controller at any time, requiring that no decision taken by or on behalf of the Data Controller that significantly impacts the Data Subject is taken by processing their personal Data solely by automated means for the purpose of evaluating matters relating to the Data Subject e.g. performance at work, creditworthiness etc. Where no notice referred to above has been given and a Data Controller makes such a decision about a Data Subject by processing their personal Data solely by automated means, then the Data Controller must inform the Data Subject that the decision was taken on such basis as soon as reasonably practicable. The University of Law does not make decisions by only automated means, therefore this right does not apply.

9.5 Rights to Correcting Inaccurate Personal Data

Accuracy of Personal Data**.**

Where personal data is inaccurate, the Data Subject concerned has a right to rectify, block, erase or destroy the inaccurate information.

If you receive a request from a Data Subject to rectify, block, erase or destroy the inaccurate information you must pass this to the DPO immediately.

10.0 Sending Personal Data outside the European Economic Area (EEA)

Personal Data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

In addition the European Commission (EC) has decided that certain other countries have an adequate level of protection of Personal Data and lists such countries on their Data Protection website.

Currently the United States of America (US) is not included on such list, but Personal Data sent to US companies who have joined the "Privacy Shield" certification scheme is considered to be adequately protected by the EC. In order to transfer Personal Data to a country that is not considered to have an adequate level of protection as set out above, certain requirements such as entering in to EC approved model contract clauses have to be met. The other principles of GDPR will also need to be considered when transferring Personal Data to different countries or territories.

Employees must always consider whether or not transfers are contractually or otherwise permissible before they send the Personal Data (especially if it crosses national borders). Where Personal Data is required to be sent abroad the DPO must be consulted to ensure that suitable checks are made regarding the legal right to do so and any security arrangements both during the transfer and whilst the Personal Data is Processed by the recipients.

For any amendments, changes or new projects that involve the transfer of data across national borders, the DPO should be consulted. The DPO can utilise the DPIA to assess the Data Protection risks.

Where there is a chance that data may be transferred outside of the EU, all relevant written agreements between ULaw and the other party must include the relevant privacy shield and/or standard clause wording.

11.0 Transfer of Data to Unaffiliated Third Parties

Any disclosure must be made in accordance with the applicable legal,l and contractual requirements and in accordance with the data protection / privacy preferences of the Data Subject. This also applies to transfers within the group. A request must be made to the DPO who will advise what requirements will be needed for approval.

12.0 Supplier Due Diligence Procedures

Due diligence procedures should be carried out during all supplier negotiations and on an ongoing basis. Roles and responsibilities for supplier data protection compliance should be clearly articulated, in order to protect Personal Data, which is the responsibility of The University of Law, maintain legal compliance and minimise operational and reputational risk.

13.0 Data Protection/Privacy Event (See Data Breach Reporting Policy)

All Employees should be vigilant of any Data Protection/Privacy Event where Personal Data has been or is at risk of exposure to an unauthorised third party, Employees must report such events to the DPO.

Below are four examples of situations where a Data Protection/Privacy Event has occurred, although other situations are possible. These types of events can be deliberate or unintentional. For specific actions that should be taken for these types of Data Protection/Privacy Events, refer to the Breaches Reporting Policy. Data Protection Officers must be aware of the different factors that determine whether or not a privacy event has occurred.

Unauthorised Access to Personal Systems Containing Personal Data

An Employee, contractor, or third party accesses a system or data they should not have access to. This unauthorised access to Personal Data can occur with either electronic (e.g. email, database, etc.) or physical information (e.g. printed materials).

Loss or Theft of Data, Media and/or Devices

Electronic (e.g., backup tapes, CDs/DVDs, external drives, laptop, mobile phone etc.) or physical information (e.g. printed materials) information is either lost or stolen by an individual or company. The information loss may occur due to the loss or theft of electronic files or physical media or devices (e.g. servers, desktops, laptops, hard disks, PDAs, mobile phones, external drives, etc.).

Inappropriate Disposal of Media and/or Devices

Physical or electronic files, media or devices are either not disposed when they are required to be or are insecurely disposed (for example, throwing sensitive documents in a standard rubbish bin) resulting in the exposure or potential exposure of Personal Data.

Improper and/or Unauthorised Communications

A mistake, incorrect process or unauthorised disclosure that results in Personal Data being communicated to an incorrect individual(s) or company (e.g., Wrong letter or email sent, incorrect name or address used, disclosure of other client account details etc.), or employee forwarding information or work emails containing another data subject's personal data to their personal email address.

14.0 Reference

Version	Date	Author	RevisionSummary
V.01	09/2019	DPO	