Data Protection and Information Security Policy

Document control

Revision History			
Version	Summary of changes	Author	Authorisation & Date
V1.0	New document	G Cooper	7th June 2018

Review	
Review due	3 years
Document location	www.liverpoolguild.org/policy O:/Policy

Contents

Introduction

Liverpool Guild of Students ("the Guild", "we", "us", "our") is fully committed to compliance with the requirements of the General Data Protection Regulation (EU) 2016/679 ("GDPR") and Data Protection Act 2018 ("DPA"). The Guild recognises in full the rights and obligations established by these laws in relation to the management and processing of personal data of students, employees and other individuals about whom we might hold information.

This policy is intended to serve as general guidance for staff and students in implementing the letter and spirit of the provision and principles of the legislation.

The Guild will therefore follow procedures that aim to ensure all members, elected officers, employees, contractors, agents, consultants or other partners of the Guild who have access to any personal data held by or on behalf of the Guild are fully aware of and abide by their duties under the GDPR and DPA.

The Chief Executive has responsibility for implementation of the Data Protection and Information Security Policy within the Guild.

Statement of Policy

In order to operate efficiently, the Guild has to collect and use information about people with whom it works. These may include the current and past members of the Guild, current, past and prospective employees, clients and customers and suppliers, and in some cases associated third parties. In addition, we may be required by law to collect and use information in the public interest or in order to comply with other legal requirements.

This personal information must be handled and dealt with properly however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the legislation to ensure this.

The Guild regards the lawful and correct treatment of personal information as paramount to its successful operations and in maintaining confidence between itself and those with whom it carries out business. The Guild will ensure that it treats personal information lawfully and correctly.

To this end, the Guild fully endorses and adheres to the principles of Data Protection as set out in section 5 of the GDPR.

Importance of Data Protection

The GDPR requires individual organisations, including the Guild, to ensure that information it holds on individuals is stored appropriately. In line with this, the Guild is registered with the Information Commissioner as a Data Controller.

The purpose of the GDPR is to protect the rights and privacy of individuals, and to ensure that data about them is not processed without their knowledge and is processed consistently with the purpose it was collected.

All staff and volunteers must be aware of the need to handle personal data in line with the GDPR and DPA, and on commencement of employment, compulsory online training via the University of Liverpool must be completed.

The Principles of Data Protection

The GDPR stipulates that anyone processing personal data must comply with the principles set out in the Regulation:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Regulation states that "*the controller shall be responsible for, and be able to demonstrate, compliance with the principles*" which are legally enforceable.

Definitions

The Regulation provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **sensitive personal** data (also called *special categories of personal data*).

Personal Data
Data which relates to a living individual who can be identified from the data, or from the data and other information about the individual which is in the possession of or is likely to come into the possession of the data controller. Personal data includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Personal Sensitive Data
Personal data relating to racial or ethnical origins, political opinions, religious beliefs, trade union membership, physical or mental health (including disabilities), sexual life, the commission or alleged commission of offences and criminal proceedings.

Data Controller
A person, or organisation, who determines the purposes for which and the manner in which any personal data, are, or are to be, processed. Data controllers are responsible for the processing of personal data by Data Processors who are processing data on their behalf.

Data Processor
Any person, or organisation, (other than an employee of the data controller) who processes the data on behalf of the data controller and was described in the Data Protection Act 1984 as a "computer bureau". Data processors have a duty to implement adequate security measures, notify the data controller of any security breaches, seek approval from the data controller to appoint sub-processors, comply with the conditions for the transfer of data outside the EEA, keep a record of categories of processing and to allow the data controller to audit and inspect their practices.

Data Subject
A living individual who is the subject of the personal data. Under the legislation this must be a natural person and may not be an association, company or other legal entity.

Processing
The collecting, recording, storing, organising, amending, retrieving, disclosure of, erasing or destroying, or otherwise using the data.

Third Party
Any person other than a data subject or the data controller or any data processor or other person authorised to process data for the data controller or processor.

Data Protection Coordinator

The Data Protection Coordinator is Graeme Cooper.

The Data Protection Coordinator can be contacted on guilddpa@liverpool.ac.uk

Notification to the Information Commissioner

The Information Commissioner's Office ("ICO") maintains a public register of data controllers. The Guild is registered as such (ICO number: Z2486502).

Data Controllers who are processing personal data are required by law to notify and renew their registration on an annual basis. Failure to do so is a criminal offence. To this end department heads will be responsible for notifying and updating the Data Protection Coordinator of the processing of personal data within their department.

The Data Protection Coordinator will review the data protection register with department heads annually, prior to notification to the Information Commissioner, revise Privacy Notices and conduct spot checks of all departments.

Any changes to the register must be notified to the ICO within 28 days; any changes made between reviews will be brought to the attention of the Data Protection Coordinator immediately.

Implementation

The Data Protection Coordinator, supported by SMT, is responsible for ensuring that the policy is implemented and will have overall responsibility for:

- The provision of cascade data protection training for staff within the Guild;
- The development of best practice guidelines;
- Carrying out compliance checks to ensure adherence, throughout the Guild, with the DPA and GDPR.

The Information the Guild stores

The Guild holds a wide range of information on individuals. This information is managed on a day-to-day basis in eleven main areas:

- Advice
- Democracy
- Facilities
- Finance
- Governance
- Human Resources
- Marketing
- Social Enterprise
- Societies & Halls Student Committees
- Student Voice
- Volunteering

As each area requires information for a different purpose, methods of collection and storage vary.

Each area therefore must appoint a member of staff who is responsible for liaising with the Data Protection Coordinator to ensure compliance with legislation. As part of this, a register will be completed at each annual review, outlining the type of data stored and the way in which legal compliance is achieved. This will be stored by the Data Protection Coordinator.

Consent

The Guild is required to obtain individual consent for some categories of *Sensitive Personal Data* and for electronic marketing. Guild staff must ensure that where consent is required it is unambiguous and freely given.

Disclosure to third parties

The Guild may appoint external organisations to process data on its behalf. When this occurs the Guild will:

a) Choose an organisation that provides sufficient guarantees in respect of the technical and organisational measures they plan to take to ensure compliance with data protection legislation;
b) Take reasonable steps to ensure compliance with those measures;
c) Enter into a written agreement that, as a minimum:
    a. Sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller;
    b. Prevents the data processor from using the data for any purpose other than under the instructions of the Guild;
    c. Sets out confidentiality requirements on personnel authorised to process personal data;
    d. Requires compliance with security measures in the GDPR;
    e. Sets limits on the appointment of sub-processors (including requiring the Guild's consent for any sub-processing);
    f. Requires the processor to assist the Guild in complying with certain GDPR obligations (such as complying with the rights of data subjects);

g. Contains provisions on the return or deletion of personal data at the end of the contract (unless the law requires otherwise);
h. Requires the processor to provide the union with all information necessary to demonstrate GDPR compliance, and contribute to audits.

Marketing

The Guild may send marketing communications to its members and non-student customers. Marketing activity is governed by the Privacy and Electronic Communications Regulations 2003 ("PECR") which require that the Guild must have consent before making any kind of marketing approach by email or telephone and this consent must have been given directly by the recipient to the Guild or its agents, or to another person in the first person (e.g. "I would like to be kept updated about the Guild's activities…").

Information provided to Members about the Guild's own activities would not normally be considered as marketing activity.

Responsibilities

General Responsibilities of Guild staff

In the course of their duties it is likely that staff will process individual personal data. When processing personal data, Guild staff must ensure that they abide by the DPA and GDPR and DPA and process data in accordance with the Data Principles. If in any doubt staff should refer to this policy, any other guidance provided or the Data Protection Coordinator.

Prior to handling any data, staff are required to have completed Data Protection and Information Security training. In addition to this staff must maintain a current knowledge of data processing best practice through refresher courses when applicable. When handling personal data staff are required to follow guidance set out by the Guild.

It is important to note that email and hardcopy exchanges between Students' Union staff and officials and other external or internal persons may have to be considered for disclosure in response to a SAR. Employees and Members must:

- keep any documented information factual and not use abusive or derogatory language in emails or other documents;
- not include any personal opinions in email or other documents;
- carry out periodic housekeeping on email and other information sources as necessary;
- keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document);
- Only copy into emails those who 'need to know';
- not use email when a telephone call will do; and
- Be aware of the Subject Access Request Procedure and Breach Procedure.

Employees must ensure that all personal data provided to the Guild is accurate and up to date. Care must be taken when collecting or entering data that it is recorded accurately.

All staff within the Guild will take steps to ensure that personal data is recorded accurately and kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of secure passwords or within restricted-access folders;
- Individual passwords should be such that they are not easily compromised.

Staff must ensure that their own details (e.g. changes of address) are updated by contacting the HR Manager.

All elected officers are to be made fully aware of this policy and their duties and responsibilities under the legislation.

Chief Executive

The Chief Executive retains ultimate responsibility for data protection at the Guild and is delegated authority by the Board to carry out their role with the resources required to be effective in the protection and security of the individual data the organisation handles.

In addition, the Chief Executive will maintain the relationship with the University of Liverpool in respect of our Data Sharing Agreement.

The Board of Trustees

The Board of Trustees has overall accountability for the strategy of the Guild and is responsible for strategic oversight of all matters related to statutory legal compliance and risk for the Guild. The Trustees should seek assurance from SMT that effective arrangements are in place and are working through the Resources & Audit Committee.

Data Protection Coordinator

The Data Protection Coordinator is responsible for:

- Informing and advising the organisation and its employees about their obligations to comply with the GDPR and other data protection laws, including the provision of cascade Data Protection training for staff within the Guild;
- Monitoring compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, training staff and conducting internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (students, employees, customers etc.).
- The development of best practice guidelines.
- Carrying out compliance checks to ensure adherence with the DPA and GDPR throughout the Guild.

Managers/Department Heads

Senior Managers are required to demonstrate ownership of the Guild's data protection policy and to communicate its values across the Guild. This accountability cannot be delegated, however operational aspects of data protection management may be delegated to other levels of management. SMT must gain assurance that these responsibilities are being fulfilled and to ensure resources are available to fulfil the requirements of this policy and associated procedures.

Managers and project leaders must ensure that staff handling data in the course of their roles have conducted the appropriate training, are processing data within the frameworks agreed and following the guidance provided. Managers are also required to conduct termly audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

Department Heads must keep the Data Protection Coordinator informed of changes in the processing of personal data in their departments and make an annual review of data with the DPC.

Students & other volunteers

Committee members, representatives and other student volunteers may handle personal data to administer their activities and services. Students handling such data are required to have completed appropriate Guild Data Protection and Information Security training prior to receiving permission to handle any personal data related to Guild activities and services. When handling personal data students are required to follow the guidance provided including the reporting of data breaches, respecting the rights of individuals and secure processing procedures. Further details can be found at www.liverpoolguild.org/privacy.

Contractors, consultants, etc.

All contractors, consultants, partners or other agents of the Guild must:

- Ensure that they and all their staff who have access to personal data held or processed for or on behalf of the Guild, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the law. Any breach of any provision of the legislation will be deemed as being a breach of any contract between the Guild and that individual, company, partner or firm;
- Allow data protection audits by the Guild of data held on its behalf (if requested);
- Indemnify the Guild against any prosecutions, claims, proceedings, actions or payments of compensation or damages without limitation.

All contractors who are users of personal information supplied by the Guild will be required to confirm that they will abide by the requirements of the law with regard to information supplied by the Guild.

Security of Data

Guild staff responsible for processing personal data must ensure that it is kept securely to avoid unauthorised access and only disclose to those authorised to receive it. Staff must ensure that they read and understand the policies and procedures relating to Information Security.

Care must be taken to ensure that PCs and terminals on which personal data is viewed are not visible to unauthorised persons, especially in public places. Screens showing personal data should not be left unattended. Staff should use the facility “lock computer” on their PC if they are absent from their desk for a short period of time and should log off if away for longer periods.

Where personal data is downloaded to local machines care must be taken to ensure that this is not accessible, for example through a PC’s downloads folder.

Registers containing Special Categories of Personal Data must be kept to a higher standard of security and access restricted strictly to those staff who require it.

The Guild’s main electronic data platform is the University of Liverpool O: Drive, which has the capacity to restrict access to sub-folders to individuals and groups. Staff and volunteers are required to store data they handle on these platforms only as detailed within the relevant guidance.

The Guild also uses online platforms, UnionCloud (online, elections, societies, volunteering), AdvicePro, Call Report and 3rings (advice). Access to information on this platform is restricted to staff and volunteers as required for their role.

Explicit permission from line management must be obtained before removing restricted information, including personal data and confidential information from Guild premises. Restricted information processed on portable devices and media must be encrypted and password protected. Media or equipment which is taken outside the Guild building must be closely secured and monitored.

In the case of hard-copy data, files containing personal data should be kept in locked storage cabinets when not in use. Procedures for booking files in and out should be used so that their movements can be tracked. Files should not be left on desks overnight.

The Guild provides facilities for the confidential destruction of paper documents. Non-routine destruction of both hard-copy and electronic records must be recorded in the Register of Processing Activities.

Handling of personal and sensitive data

The Guild will, through appropriate management and the use of strict criteria and controls:

- observe fully conditions regarding the fair collection and use of personal information;
- collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ensure the quality of information used;
- apply strict checks to determine the length of time information is held;
- take appropriate technical and organisational security measures to safeguard personal information
- ensure that personal information is not transferred outside the EEA without suitable safeguards; and

- ensure that the rights of people about whom the information is held can be fully exercised under the law. These include:
  - The right to be information that processing is being undertaken;
  - The right to access your personal information;
  - The right to prevent processing in certain circumstances;
  - The right to correct, rectify, block or erase information regarded as wrong information.

In addition, the Guild will ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are dealt with promptly and courteously;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance with handling personal information is regularly assessed and evaluated; and

- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

IT Systems

Employees and volunteers must undertake the Information Security course provided by the University of Liverpool to ensure sufficient security awareness. Department-specific training will also be provided. Employees and volunteers must make best efforts to protect their user accounts by using a strong password. Account usernames and passwords should not be shared.

Digital equipment and media containing information must be secured against theft, loss or unauthorised access by the appropriate use of passwords and encryption. In addition, all digital equipment and media must be disposed of securely and safely when no longer required.

Third Party Contracts

Occasionally the Guild may transfer data to third parties for processing, prior to data transfer a contract or data sharing agreement to ensure compliance with relevant legislation must be in place.

Where the Guild is appointing a Sub-Processor for data of which the Guild is a Processor, the data controller must be informed and provide written consent to the arrangement.

Compliance

Right to be Informed (Privacy Notices and Fair Processing Statements)

A data protection statement (or Privacy Notice) must be included or referenced on all forms capturing personal data, within guidance notes for the completion of forms, in relevant staff and student handbooks, and on any forms completed online.

The Guild will publish on its website, and make available when necessary, such Privacy Notices as required for each category of data subject to include the required fair processing statements.

These will include fair processing statements describing where we collect data, what data we collect, the lawful basis for processing that data, the retention policy, how we keep the data secure and details of the data subject's rights and responsibility to keep the data current.

Where personal data is collected the individual should be directed to the relevant Privacy Notice. General Privacy Notices will be produced for likely users of the Guild however specific Privacy Notices should be considered where there are unusual circumstances. These notices should be reviewed annually and must be updated more frequently if changes to processing require. If in doubt the Data Protection Coordinator should be consulted.

Right of Subject Access

The GDPR gives data subjects the right to access their personal data to verify the lawfulness of the processing. This entitles the individual to be told by the Guild whether they are processing that individual's personal data, the purposes for which it is being processed, to whom they are or may be disclosed and to receive in an intelligible manner, a copy of their personal data. If the response is provided electronically the data should be provided in a commonly used electronic format.

The Guild is required by law to respond as quickly as possible, but usually within one month of receipt of the request. The time limitation may be extended by a further two months where requests are numerous or complex. Where the time limitation is extended the individual must be informed within one month of receipt of the request with an explanation as to why the extension is necessary.

If the request arises as part of another matter for instance a complaint, grievance of disciplinary matter, the requirements of the law must not be overlooked, particularly the one month deadline. In these circumstances staff must seek advice from the Data Protection Coordinator.

This information must usually be made free of charge however where requests are 'manifestly unfounded or excessive, in particular because they are repetitive', the Guild may:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where a request is refused, the Guild will explain why to the individual informing them of their right to complain to the ICO.

The Guild will publish guidance on how to access your personal data and a Subject Access Request form to be used, and a procedure for staff on the handling of requests for personal data.

In all cases, the Guild must ensure that it has sufficient proof of the identity of the requestor to prevent an unlawful disclosure.

A data subject can request access to their personal data through another party such as a lawyer or an advocate. A signed letter or form of authority from the data subject must be provided before any data is disclosed.

Third Party Data and the Subject Access Right

When handling a subject access request, sometimes another individual (known as a third party) may be identified in the personal data to be disclosed. The Guild will only disclose third party data with the consent of that third party, or if it is reasonable to do so without consent. In determining whether it would be reasonable, the Guild must balance its duty of confidentiality to the third party against the rights of the data subject, consider any steps taken to seek consent, whether the third party is capable of giving consent, or any express refusal of consent by the third party.

Data Rectification, Restriction, Objection or Erasure

If the data subject believes that their personal data is inaccurate, out of date, held unnecessarily or is offensive, they have the right to have the information rectified, blocked, erased or destroyed. The data subject also has the right to insist that the Guild ceases to process their personal data if such processing is causing or is likely to cause unwarranted substantial damage or substantial stress to them or to another.

The Guild will not unreasonably prevent erasure, objection, restriction or rectification of data however we require an appropriate reason to make such amendments. There may be cases where the Guild must retain some or all of the data subject to these requests in which case we will note the request and comments in the appropriate record.

Erasure of data may result in restrictions on the use of the Guild's services as we are required to process certain data to deliver those services.

Complete erasure of all data will result in revocation of Guild Membership; it may also be necessary to retain details some personal data to ensure the Guild does not process any data associated with these records.

Exemptions

There are a number of exemptions from the provisions of the legislation. These allow the Guild to either disclose or withhold data from disclosure in particular circumstances, without breaching the data protection principles.

Breach Management

Guidance for staff setting out the procedures to follow once a data protection breach has been identified and is set out in the *Data Breach Procedure*.

All breaches must be notified to the Data Protection Coordinator. If the breach is sufficiently serious the DPC will decide whether the ICO or Data Subjects must be informed.

Data Protection by Design

Employees and volunteers are required to adopt a privacy by design approach to planning data collection and processing. In addition to data collection records, Data Protection Impact Assessments ("DPIAs"), Privacy Impact Assessments ("PIAs") and where appropriate Legitimate Interest Assessments ("LIAs") shall be completed prior to any data collection or processing. Information on conducted PIAs and LIAs are available from the Data Protection Coordinator.

Data Protection Impact Assessments

Data Protection Impact Assessments are a tool which can help organisations to identify the most effective way to comply with their data protection obligations and meet individual's expectations of privacy. The Guild will undertake DPIAs when using new technologies or when processing data is likely to result in a high risk to the rights and freedoms of individuals (such as large-scale processing of sensitive data).

A DPIA should contain a description of the processing operations and purposes, including, where applicable, the legitimate interests pursued by the controller; an assessment of the necessity and proportionality of the processing in relation to the purpose; an assessment of the risks to individuals; and the measures in place to address risk, including security and to demonstrate that you comply. A DPIA can address more than one project.

Guidelines on high risk processing and DPIAs can be found here:
http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Children

Guild staff and volunteers shall not ordinarily process data related to any individual under the age of 16. Should a situation arise requiring the storage of data relating to anyone under 16 years of age the Data Protection Coordinator should be consulted to ensure compliance with relevant legislation.

Data Protection Advice

Any questions or concerns about the interpretation or operation of this policy should be referred to the Data Protection Coordinator.

Guild staff should not seek external legal advice directly from the Guild's lawyers or data protection advice from any other sources, without first consulting with the Data Protection Coordinator.

The Information Commissioner

The Information Commissioner is an independent official appointed by the Government to oversee the Data Protection Act 2018, General Data Protection Regulation (EU) 2016/679, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. The Commissioner

reports annually to Parliament. The Commissioner's decisions are subject to the supervision of the Courts and the Information Tribunal.

The Information Commissioner provides good practice guidance and interpretation of the law for data controllers and advice to the public on how to access personal data. The website of the ICO is http://www.ico.org.uk

The Commission has formal powers to force a data controller to take or refrain from certain actions if the Commissioner has determined there has been or is likely to be a breach of the legislation. Failure to comply with a Decision or an Enforcement Notice may be dealt with as Contempt of Court. From the implementation of GDPR the Commissioner has been able to impose fines of up to **€20,000,000** penalty for serious breaches of the legislation.

Policy Monitoring

A Data Protection Overview Group, consisting of the Chief Executive, Senior Managers and Data Protection Coordinator, will monitor compliance with the policies and procedures laid down in this document. The Data Protection Overview Group will provide reports to the Resources & Audit Committee.

The Data Protection Coordinator is responsible for the monitoring, revision and updating of this policy and appendices 2, 4 & 5, on a three-yearly basis or sooner if required.

The Chief Executive is responsible for the review of Appendix 1a jointly with the University of Liverpool, as required.

The Director of Marketing is responsible for the review of Appendix 3 as required.

Data Protection at the University of Liverpool

Full details of the University's Data Protection Policy and supporting documents can be found at https://www.liverpool.ac.uk/legal/data_protection/.

Schedule of Appendices

	Title	**Location**
1	Data Sharing Agreement with a) the University of Liverpool	Available from Student Administration and Support Division
2	Privacy Notices a) Students i) Advice Centre Users b) Employees i) Job Candidates c) Consumers d) Clients, Contractors and Suppliers e) Third Parties	www.liverpoolguild.org/privacy
3	Cookies Statement	www.liverpoolguild.org/get_cookie_policy_details
4	Data Subject Access Request Procedure a) SAR Form	O:/Policy/ www.liverpoolguild.org/privacy
5	Data Breach Procedure	O:/Policy/