Liverpool Guild of Students

Liverpool Guild of Students
160 Mount Pleasant, L3 5TR
+44 (0) 151 794 6868
www.liverpoolguild.org

Charity Number: 1137398
Company Number: 07324992

Data Protection and Information Security Policy

Approval Date	8th July 2024	**Expiry Date**	8th July 2027
Approved by	Resources & Audit		
Review Frequency	Three Years		
Policy Code	G034		

Review History		
Date	**Name**	**Comments**
08/07/2024	A Middleton	Full review
14/09/2018	G Cooper	Adds use of Google G Suite & appendices list
07/06/2018	G Cooper	New policy

Table of Contents

1. Introduction

Liverpool Guild of Students ("the Guild", "we", "us", "our") is fully committed to compliance with the requirements of the UK General Data Protection Regulation ("UK 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.

1.1. Purpose & Scope

The policy is produced for several key purposes and is intended to be read by both staff and members who handle personal data in their roles at the Guild.

a) It gives an overview of how data protection applies and areas of data protection that they must be aware of whilst in their role.

b) This policy gives practical advice about what to do in specific situations.

c) It makes staff and members aware of the Guild's commitment to data protection compliance and explains where to obtain further advice and information where necessary.

d) This policy has been approved by the Guild's Resources & Audit Committee. Any breach of this policy will be taken seriously and may result in disciplinary proceedings.

e) Any individual who considers that the policy has not been followed in respect of their personal data should raise the matter with the Guild's Data Protection Coordinator, in the first instance. It is a mandatory requirement to report any serious data breaches to the Information Commissioner's Office within 72 hours. These should be reported immediately to the Data Protection Coordinator.

1.2. 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 Data 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 Data 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 Data 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 UK GDPR.

1.3. Importance of Data Protection

The UK 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 UK 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 members must be aware of the need to handle Personal Data in line with the UK GDPR and DPA. This policy details how to handle Personal Data as a staff member and also refers to members who handle Personal Data in Guild roles such as committee members, representatives and other student volunteers.

2. The Principles of Data Protection

Data protection is a principle-based law, meaning that there are a number of guiding principles that the Guild must meet. These principles guide how we handle personal data and each principle must be met completely.

The data protection principles state that personal data shall be:

- Processed fairly, lawfully and in a transparent way.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary, kept up to date.
- Kept for no longer than is necessary.
- Kept secure.

The UK GDPR also includes a responsibility for the Guild to document and demonstrate how it complies with the law.

2.1. How the Principles Apply

The Guild has a responsibility to ensure that its staff and members are aware of the data protection principles and ensure they are always followed. Data protection applies to all types of personal data held by the Guild, whether they are paper based or electronic.

Principle 1 – Fair, Lawful and Transparent

Fair and Lawful

The Guild must always ensure its use of personal data is both fair and lawful.

Fair means that we must consider whether our use of personal data may affect individuals and consider any adverse impact on them. It also means that we are open and honest with them through our privacy notices about how their data is used.

Lawful means that the Guild does not use personal data for any unlawful purposes and that personal data is not used to break either data protection or any other law of the land. This could include a breach of confidence, the Human Rights Act or copyright.

Lawful also requires the Guild to identify a legal basis within the UK GDPR for its use of personal data. The UK GDPR contains six lawful bases. One of them must be applied to every function that requires the use of personal data.

The lawful bases are:

Consent– The individual has given their clear agreement for the Guild to use their data for the purpose.

Contract– The use of personal data is necessary for a contract we have with the individual or steps we are taking to enter into a contract with them. This is the most common legal basis for HR activity.

Legal Obligation– The use of personal data is necessary for the Guild to comply with the law. This could be a statutory obligation or a court order.

Vital Interests– The use of personal data is necessary to protect someone's life. This is usually a life or death situation.

Public Task– The use of personal data is necessary to provide a task in the public interest or is in line with a power in law.

Legitimate Interests– The use of personal data is necessary to support the legitimate interests of the Guild or a third party. This condition also states that the Guild must not use information in this way if it will compromise the rights or freedoms of the person who the data is about.

Transparent

When using personal data, the Guild must be open and clear about what the data will be used for and how it will be used. The UK GDPR requires Guild to provide a wide range of information to the person whose data we are using. This is done through privacy notices.

Principle 2 – Collected for a Specific Purpose

The Guild must ensure that it collects personal data for clear, appropriate and legitimate purposes. Collecting personal data "just in case" for future reference is not compliant with the legislation.

Through our privacy notices we must communicate our purposes to individuals when we collect their data in a clear way. If you feel the need to hide a purpose from the individual, perhaps we shouldn't be collecting personal data for it.

Whilst the UK GDPR state the Guild must only use personal data for the purposes we specify, it may also re-use that data for compatible purposes. Where you are re-using personal data for a new purpose, the Data Protection Coordinator will advise if this is appropriate.

Principle 3 – Adequate, Relevant and Limited to what is necessary

The Guild must only use, collect or share personal data in a proportionate way. This means that it should collect what it needs to complete its purposes but nothing more than that.

For example, if we need to collect a student's name and address for the purpose, that is all we should collect. It might be nice to know their eye colour and their favourite band, but if we don't need it to complete the purpose, we shouldn't collect it.

Principle 4 – Accurate and Up to Date

Personal data must be accurate and up to date. Inaccurate information is one of the key contributors to data protection incidents.

Collecting inaccurate data is an automatic breach of the UK GDPR. Where inaccuracies are identified, they must be rectified as soon as possible and as many steps taken as possible to ensure the correct information is updated on Guild systems.

Principle 5 – Kept No Longer Than Is Necessary

Personal data must only be kept for a specific period of time. This time period will vary depending on what purpose the personal data is collected for. The Guild Retention Schedule details how long personal data should be kept for each function.

Principle 6 – Stored Securely

The UK GDPR states that the Guild must take appropriate "technical and organisational" measures to keep the personal data that we hold in a secure way. This does not only apply to personal data held electronically, it also applies to physical documents that hold personal data.

3. Definitions

Personal Data
Personal data is information that either on its own, or when combined with other information, can identify a living individual.

This can include (but is not limited to):

Names, addresses, student and staff ID numbers, dates of birth, photographs, social media handles, video footage, emails and WhatsApp messages.

Personal data has a very wide definition and can include descriptions, personal opinions, and intentions. For example, a man sat with a group of women can be identified by the fact that he is male. This statement alone is enough to identify him and therefore is personal data.

The main types of personal data that the Guild uses are staff and student data (prospective, current, and alumni).

Special Category Data
Certain types of personal data are deemed more sensitive than others. Personal data that falls into the following categories is called special category data. These categories of data require extra safeguards to be met when they are used.

Personal data that fall into the special categories are related to:

- Race or ethnic origin
- Political opinions

- Religious or philosophical beliefs
- Trade Union Membership
- Genetic data
- Biometric data
- Health data (either physical or mental health)
- Sex life or sexual orientation

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.

Data Controller
An organisation or individual that decides how and why personal data is collected and used is called a Data Controller. Data Controllers are responsible for all areas of complying with data protection legislation and must also register with the Information Commissioner's Office (the regulator for information law). The Guild's registration number is Z2486502. The Guild is a Data Controller.

Data Processor
Data protection legislation refers to the processing of personal data. Processing simply means any use of personal data. This can range from collecting it to sharing it, from amending it to deleting it. The Guild is a Data Processor of student data that we receive from the University.

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

Subject Access Request (SAR)
A subject access request (SAR) made by a Data Subject in accordance with UK GDPR.

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.

4. Data Protection Coordinator

The Data Protection Coordinator is Alice Middleton, Governance Manager.

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

4.1. 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 the Senior Leadership Team (SLT) 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 SLT 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.

5. Implementation

The Data Protection Coordinator, supported by SLT, 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 UK GDPR.

6. Data Sharing with the University

The Guild and University of Liverpool have a Data Sharing Agreement (DSA) which should be read in conjunction with this policy. The relationship can be summarised as follows:

- The Guild (Data Processor) receives access to University of Liverpool students Personal Data (Data Controller) in order for the Guild to carry out its activities (detailed in the DSA)
- The University of Liverpool (Data Processor) receives access to Guild employee's Personal Data (Data Controller) in order to undertake payroll duties

Staff should be familiar with the data they handle in relation to their role and should work with their line manager to ensure full understanding.

7. 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 (HR)
- 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 is kept, outlining the type of data stored and the way in which legal compliance is achieved. This will be maintained by the Data Protection Coordinator.

7.1. Consent

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

7.2. 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 UK 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 UK 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 UK GDPR compliance and contribute to audits.

7.3. 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.

A Data Subject's objection to direct marketing must always be promptly honoured. If an individual opts out of marketing at any time, their details should be suppressed as soon as

possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

8. Responsibilities

8.1. 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 UK GDPR and process data in accordance with the Data Principles. Staff should be familiar with the data they handle in relation to their role and should work with their line manager to ensure full understanding. If in any doubt staff should refer to this policy, any other guidance provided or the Data Protection Coordinator.

Training - 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 handling best practice through refresher courses when applicable and with the guidance of their line manager. When handling Personal Data staff are required to follow guidance set out by the Guild.

Staff should follow the practical security tips outlined in this policy to ensure information is kept securely.

Staff must ensure that their own details are updated in the Guild's HR software - Staff Savvy. Staff should also notify Guild HR separately of a change in bank details.

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

8.2. Chief Executive Officer (CEO)

The CEO 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 CEO will maintain the relationship with the University of Liverpool in respect of our Data Sharing Agreement.

8.3. 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 SLT that effective arrangements are in place and are working through the Resources & Audit Committee.

8.4. 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 UK GDPR and other data protection laws, including the provision of cascade data protection training for staff within the Guild;

- Monitoring compliance with the UK 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 UK GDPR throughout the Guild.

8.5. Senior Leadership Team (SLT)

The SLT 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. SLT 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 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 audits of their relevant spaces and IT infrastructure to identify weaknesses in information security.

SLT must keep the Data Protection Coordinator informed of changes in the processing of Personal Data in their departments.

8.6. Members in voluntary Guild roles

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 https://www.liverpoolguild.org/about/privacy/.

8.7. Contractors, Consultants, Partners or other agents

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 Data 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.

9. Information Security

Those 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 and members must ensure that they read and understand the policies and procedures relating to Information Security.

9.1. IT Systems

In accordance with the Guild's Memorandum of Understanding (MOU) with the University the Guild has access to the University's Managed Windows System (MWS). All staff should have MWS accounts which must be used in accordance with the University's IT Acceptable Use Policy.

The Guild's main electronic data storage platforms are the University of Liverpool O: Drive and Microsoft Teams sites, which have the capacity to restrict access to sub-folders to individuals and groups. Staff and members are required to store data they handle on these platforms only as detailed within the relevant guidance.

The Guild also uses other platforms and software detailed in the Record of Procession Activity. Access to the platforms and software is restricted as required for roles.

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.

Using Guild Systems

- Just because you have access to a system, this does not mean you have the right to access all of the information on it. Access is on a "need to know" basis.
- "Curiosity" checks are not permitted. You must have a genuine, legitimate purpose to access information
- Never share passwords. If a colleague or member forgets their password, they need to have it reset by IT. Do not let them access a system under your username.
- Any information you access on a system will be logged. Do not let anyone else use your computer to retrieve information and do not undertake requests on their behalf.
- Always be professional when using Guild systems. Do not input anything derogatory, inappropriate or rude about individuals.
- If you have been provided with a Guild device for your role ensure that this is used rather than your own personal devices.

9.2. Practical security tips

Using personal data in a safe and secure way does not need to be complicated. All staff and members are reminded to follow the points below when they are accessing Guild systems and refer to this policy first or ask for advice from the Data Protection Coordinator if they are unsure of how to proceed.

- Care must be taken to ensure that devices (PCs, laptops, tablets, tills etc) on which Personal Data is viewed are not visible to unauthorised persons, especially in public places.
- Always lock your screen when you leave your desk. This avoids leaving your systems open to access and also stops those nearby reading any personal data you may have left on screen.
- Remember that the Guild is an open building and to keep Personal Data stored away securely and not in view of the public. Ensure that offices are locked when empty and ensure that confidential conversations are not overheard in the building.
- Clear documents away at the end of the day or when leaving your desk. This stops people who are walking past your desk from reading things they shouldn't.
- Store paper documents that contain Personal Data in locked storage cabinets when not in use. Use a procedure for booking files in and out if necessary.
- Double check when entering information into Guild systems. Taking the time to check addresses and phone numbers is a vital part of data handling.
- Double check addresses when sending emails. It is easy to mistype or click the wrong name on Outlook. Once the email has gone, it cannot be retrieved. Take the time to get the recipient right before you press send. Remember BCC if you need it.
- When taking information out of the office, think about the most appropriate way to do so. Guild provided MWS laptops are encrypted and difficult to access if they are lost. Paper documents are not as secure as they can be read by anyone who finds them.
- Don't print unless you have to and collect your printing immediately.
- The Guild provides facilities for the confidential destruction of paper documents.
- If you are regularly sending personal information to organisations outside of the Guild and University, ensure that you verify who you are contacting and password protect the document if necessary.
- Where possible avoid using names and other identifiers in email subject headings and meeting/calendar requests.
- Take care when working from home. Your family members don't have a right to see the information you use for work.
- Don't leave equipment or documents in your car overnight if you need to take them home. You wouldn't leave your own laptop on the front seat of your car, so don't leave your work one there either.

It is important to note that email and hardcopy exchanges between staff or members 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 SAR 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 (SAR) Procedure and Breach Procedure.

9.3. 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 Data;
- 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 Data;
- ensure that Personal Data 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 Data;
  - 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 Data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling Personal Data is appropriately trained to do so;
- Everyone managing and handling Personal Data is appropriately supervised;
- Anyone wanting to make enquiries about handling Personal Data, whether a member of staff or a member of the public, knows what to do;
- Queries about handling Personal Data are dealt with promptly and courteously;
- Methods of handling Personal Data are regularly assessed and evaluated;
- Performance with handling Personal Data 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.

9.4. 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 Data Processor, the Data Controller must be informed and provide written consent to the arrangement.

10. Compliance

10.1. 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.

10.2. Right of Subject Access

The UK 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 (SAR) 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.

10.2.1. 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.

10.3. 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.

10.4. 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.

10.5. 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 Data Protection Coordinator will decide whether the ICO or Data Subjects must be informed.

10.6. Data Protection by Design

Employees and members 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.

10.7. Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessments (DPIAs) 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) including:

a) Use of new technologies (programs, systems or processes, including the use of AI), or changing technologies (programs, systems or processes).

b) Automated Processing including profiling.

c) Large-scale Processing of Personal Sensitive Data of Personal Data or criminal convictions data.

d) Large-scale, systematic monitoring of a publicly accessible area

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. Further advice in relation to conducting a DPIA can be sought from the Data Protection Coordinator.

10.8. Children

Guild staff and members 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.

10.9. 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.

10.10. The Information Commissioner (ICO)

The Information Commissioner (ICO) 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 UK GDPR the Commissioner has been able to impose fines of up to **€20,000,000** penalty for serious breaches of the legislation.

11. Policy Monitoring

A Data Protection Overview Group, consisting of the Chief Executive, SLT and the 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, SLT and staff responsible for areas of data are responsible for the monitoring, revision and updating of this policy and appendices, on a three-yearly basis or sooner if required.

12. 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/.

13. Schedule of Appendices

	Title	Location	Staff Responsible
1	Data Sharing Agreement (DSA) with the University of Liverpool	Guild Departmental O Drive	CEO
2	University's IT Acceptable Use Policy	https://www.liverpool.ac.uk/media/livacuk/computingservices/regulations/IT_Acceptable_Use_Policy.pdf	University
3	Privacy Notices	https://www.liverpoolguild.org/about/privacy/	Data Protection Coordinator
4	Cookies Statement	https://www.liverpoolguild.org/cookies/	Director of Business Development

5	Data Subject Access Request Procedure a) SAR Form	https://www.liverpoolguild.org/about/privacy/	Data Protection Coordinator
6	Data Breach Procedure	Guild Departmental O Drive	Data Protection Coordinator
7	Record of Processing Activity	Guild Departmental O Drive	Data Protection Coordinator
8	Guild Retention Schedule	Guild Departmental O Drive	Data Protection Coordinator
9	Data Register	Guild Departmental O Drive	Data Protection Coordinator