The Worshipful Company of Grocers - Data Protection Policy

Document name	Data Protection Policy
Version number	3.0
Department or Team	Compliance Manager
Relevant policies	Grocers' Hall CCTV Privacy Notice
Associated Documents	Annex A – The Worshipful Company of Grocers Data Audit dated 22-Jan-2025
Distribution	Internal and External upon request
Author / Owner	DPO, Eddie Walsh, eddie@grocershall.co.uk
Approved by	SIRO - Brigadier Greville Bibby CBE
Date of sign off	26/02/2025
Reviewed by	31/01/2026

1. **Key messages**

   a. The purpose of this document is to outline:

      (1). How the Worshipful Company of Grocers, the Grocers' Charity and the Grocers' Retirement Benefits Plan (the '**Company**'), will ensure compliance with the UK GDPR and Data Protection Act 2018.

      (2). Explain the roles and responsibilities relevant to internal compliance.

      (3). How compliance with this policy will be monitored.

   b. This policy applies to all processing of personal data carried out by the Company including processing carried out by controllers, contractors and processors.

2. **Table of Contents:**

- Introduction.
- Background.

- Information Covered by Data Protection Legislation.
- Key Concepts and Definitions of Applicable Data Protection Law.
- The Data Protection Principles.
- Data Subjects' Rights.
- Our Commitment and Additional Requirements.
- Roles and Responsibilities.
- Other Roles.
- Monitoring.
- Feedback on this document.
- Version history.

3. **Introduction**

a. This policy provides a framework for ensuring that the Company meets its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18).

b. The Company complies with data protection legislation guided by the six data protection principles. In summary, they require that personal data is:

(1). processed fairly, lawfully and in a transparent manner.

(2). used only for limited, specified stated purposes and not used or disclosed in any way incompatible with those purposes.

(3). adequate, relevant, and limited to what is necessary.

(4). accurate and, where necessary, up to date.

(5). not kept for longer than necessary; and

(6). kept safe and secure.

c. In addition, the accountability principle requires us to be able to evidence our compliance with the above six principles and make sure that we do not put individuals at risk because of processing their personal data. Failure to do so, can result in breach of legislation, reputational damage, or financial implications due to fines. To meet our obligations, we put in place appropriate and effective measures to make sure we comply with data protection law.

d. The Company will not keep personal data for longer than is necessary for the purposes for which the data are processed. The duration for which personal data are stored will be dictated

by applicable legal, business or other reasons, such as retention periods driven by tax legislation (currently 7 years).

e. If the Company cannot establish a valid legal, business or other reason for retaining personal data, it will be securely deleted. The Company will specify the periods for which personal data are stored after the storage period has expired, personal data will be deleted (see Annex A, column d).

f. The Company may store some categories of personal data for longer periods where such processing is solely for archiving purposes in the public interest, or historical research purposes. In such cases, the Company must implement appropriate safeguards, such as allowing data subjects to request deletion of some of their personal data.

g. Our staff have access to this policy and receive regular guidance to give them appropriate direction on the application of the data protection legislation.

4. **Background**

a. While running its day-to-day business and promoting its charitable and educational aims, the Company, may collect and process information about its members and staff as well as members of the public such as enquirers and correspondents.

b. This policy does not document every part of the Data Protection Legislation which may be relevant but merely focuses on the key aspects that are likely to be applicable to the Company. Should other issues arise in practice not covered by this policy, the Company will consider these separately at the time. The Company will review this policy annually and may amend it from time to time as it sees fit.

c. The Company regularly processes the following categories of personal data:

(1). **Staff**: The Company has a small number of employees, about whom it holds personal data such as employment history, education and qualifications, and identifiers such as photographs, contact details and record of employment with the Company. The Company may process information about its employees' health or medical details. The Company processes such employee personal data for ordinary staff administration purposes, including salary payment and conferring other benefits, conducting appraisals, training and management. It also collects personal data about prospective candidates in the recruitment process. The Company holds some information about its employees and former employees for pension purposes, and archival and historical research purposes, for example, to maintain a roll of past Clerks and Beadles.

(2). **Members**: The Company holds the personal data of its past, present and prospective members (Liverymen, Freemen, and Probationers). The personal data held includes members' education and employment history, qualifications, photograps, hobbies and interests, personal and family circumstances, as well as financial and contact details and essential medical and health details for members' own safety. The Company processes such personal data in order to administer membership, to organise events such as meetings and social events, and to collect subscription fees. It also processes members' personal data for fundraising purposes including seeking endowments such as gifts, trusts and bequests. The Company holds some information about its members

for archival and historical research purposes, for example, to maintain a roll of past Masters, Liverymen and Freemen.

(3). **Beneficiaries**: The Company's charitable and educational activities have been an integral part of its operation throughout its history. In order to further its charitable and educational aims, the Company may process personal data about beneficiaries and potential beneficiaries, which may include personal, family and financial circumstances, education, and employment history as well as photographs. The Company may also process personal data about its beneficiaries for historical and archiving purposes.

(4). **The public**: The Company may enter into correspondence with members of the public, such as enquirers, correspondents. When it does so, the Company may collect incidental personal data such as contact details and personal circumstances and processes such personal data in order to respond to queries and deal with ad hoc issues.

(5). **Clients**: The Company processes personal data concerning its clients of Lent Hall[1], including identifiers such as contact details, financial information, insurance information, credit history and photographs. The Company processes such information in order to provide quotes, write contracts, produce invoices and marketing.

(6). **Suppliers**: The Company processes personal data concerning its suppliers of goods and services, including identifiers such as contact details, financial information, insurance information and purchase history. The Company processes such information in order to purchase goods and services, to pay its suppliers and to maintain its accounts and records.

5. **Information Covered by Data Protection Legislation**

a. The UK GDPR definition of "personal data" includes any information relating to an identified or identifiable natural living person.

b. Pseudonymised personal data is covered by the legislation, however anonymised data is not regulated by the UK GDPR or DPA 18, providing the anonymisation has not been done in a reversible way.

c. Some personal data is more sensitive and is afforded more protection, this is information related to:

(1). Race or ethnic origin.

(2). Political opinions.

(3). Religious or philosophical beliefs.

(4). Trade union membership.

(5). Genetic data.

[1] Lent Hall is a term used within Grocers' Hall to indicate a Commercial Venue Hire.

(6). Biometric ID data.

(7). Health data.

(8). Sexual life and/or sexual orientation; and

(9). Criminal data (convictions and offences).

6. **Key Concepts and Definitions of Applicable Data Protection Law**

a. '***Personal data***' means any information relating to an identified or identifiable natural person (a 'data subject', which is explained in more detail below). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the identity of that natural person.

The Company will hold personal data about its past, present and prospective members (including Liverymen and Freemen) staff and members of the public such as beneficiaries, as well as its suppliers. The Company may hold such personal data both in electronic and hard copy format, in records, correspondence and minutes.

b. '***Processing***' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing is interpreted very broadly, so that almost all activities organisations carry out in relation to their personal data are captured by the definition.

The Company will generally be deemed to be processing any personal data that it may collect, record, store and/or disclose.

- *And* ***'Processing by third parties'*** for the most part, personal data collected by the Company will remain within the Company and will be processed by appropriate individuals only in accordance with a 'need to know' basis. However, some functions are outsourced including (but not limited to) cloud storage, Diligent, Momentus Technologies, Naked Creativity, Sage, Sage HR, Salesforce, Stripe, Tela, and Thinkscape. Third party processing may include joint access to ensure efficiency as follows:

    - Tela and Naked Creativity have access to Priava (becoming Momentus) to assist with IT related issues and processes.
    - Naked Creativity also have access to Salesforce to maintain and administer the Members area.
    - Nimbus Point have access to Salesforce as they have implemented the system for us (this is wider than Lent Hall, and involves the Company and Charity)

In accordance with Data Protection Law, this type of external data processing is always subject to contractual assurances that personal data will be kept securely and used only in accordance with the Company's specific directions.

c. '*Controller*' means the natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data. The Data Protection Legislation applies to controllers, who must comply with its requirements.

   The Company will generally be a controller in relation to the personal data of its members, staff, members of the public such as beneficiaries and enquirers, and suppliers.

d. '*Processor*' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Where a controller uses a processor to process personal data on its behalf, the controller must only use a processor that provides sufficient guarantees to ensure that personal data is processed securely, and in accordance with the requirements of the GDPR. Controllers must engage processors by way of a contract incorporating the provisions specified by Article 28 of the GDPR.

   The Company may use processors for a variety of purposes; for instance, to store personal data, to send email communications, or to calculate staff payroll. In each case, it must have conducted sufficient due diligence to be able to evaluate whether the processor offers sufficient guarantees to protect personal data and must ensure that the processor is bound by a contract that incorporates the provisions specified by the GDPR.

e. '*Special categories of personal data*' means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic or biometric data, data concerning health (including medical data, and medical records, for example), or concerning an individual's sex life or sexual orientation.

   The special categories of personal data require a higher standard of care. If a personal data breach (as defined below) occurs that involves the loss of any of the special categories of personal data, the ICO will regard this as a serious breach. The GDPR also requires that personal data relating to criminal convictions and offences is treated with a higher standard of care.

   The Company does not hold a significant volume of the special categories of personal data, though in the event that it does, it will ensure the information is handled accordingly.

f. '*Data subject*' means an individual to whom personal data relate. Typically, these are employees, customers, and suppliers.

   The categories of data subject whose personal data the Company is likely to process will include members, staff, suppliers and members of the public.

g. '*Personal data breach'* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

   A personal data breach may be accidental, such as a system failure, or loss of an electronic or physical file, or malicious, such as a cyberattack. In the event that the Company suffers a personal data breach, it must take specific steps, explained below in this policy.

7. **The Data Protection Principles**

The data protection principles are standards which the Company must observe when processing personal data. These principles are as follows:

a. **Fairness, lawfulness and transparency**

This is the most important of the data protection principles and comprises three elements: fairness, lawfulness and transparency. Considering these in more detail:

(1). **Fairness:** Organisations generally cannot process individuals' personal data in a way that an individual would not have reasonably expected. Collecting personal data on the pretext of one purpose and then using it for another, unrelated purpose is unlikely to be fair. The Company should consider whether its uses of personal data would fall within the reasonable expectations of the affected data subjects.

(2). **Transparency:** Organisations must provide certain prescribed information to individuals when processing their personal data, including the organisation's identity, the purposes for which personal data are being processed, or are to be processed, and any third-party recipients of the personal data. A complete list of the information that must be provided to data subjects can be found in Articles 13 and 14 of the GDPR. The transparency information must accurately reflect the controller's use of personal data. This is frequently provided by way of a website privacy notice but may also be provided by way of a disclaimer on a paper form, or a pre-recorded message in the context of recorded telephone calls.

The Company publishes this Data Protection Policy to ensure it is available on the website, and any other means by which it makes the transparency information available to data subjects (such as a disclaimer on a paper form). This accurately and comprehensively reflect its processing activities.

(3). **Lawfulness:** Organisations must establish at least one of a number of lawful grounds for processing. These lawful grounds are set out in Article 6 of the GDPR and are as follows:

(a). The data subject has given his or her **consent** to the processing.

(b). Processing is necessary for the **performance of a contract**.

(c). Processing is necessary for **compliance with a legal obligation** to which the controller is subject.

(d). Processing is necessary in order to protect the **vital interests of the data subject** or of another person.

(e). Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the controller.

(f). Processing is necessary for the purposes of **legitimate interests** pursued by the controller or by a third party.

In practice, the Company will frequently be able to rely on the second and sixth grounds (performance of a contract, and the legitimate interests ground) for many of its activities. Note that the grounds for processing the special categories of personal data are different.

b. **Purpose limitation**

This principle requires that the purposes for which personal data are processed are limited to those purposes specified in the transparency information that has been provided to the affected data subjects, and not processed for any further, incompatible purposes. Note that any further processing operations for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible purposes.

The Company should only process personal data it holds for those purposes specified in the website Data Privacy Policy.

c. **Data minimisation**

Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The Company should only collect the personal data that is strictly necessary for the purpose for which it was collected, and should not collect additional, unnecessary personal data on a 'just in case' basis.

d. **Accuracy**

Personal data must be kept accurate, and up to date.

The Company must ensure that any requests from data subjects to update their personal data are dealt with promptly, having satisfied itself as to the requester's identity.

e. **Storage limitation**

Personal data must not be kept for longer than is necessary for the purposes for which the data are processed. The duration for which personal data are stored will be dictated by applicable legal, business or other reasons, such as retention periods driven by tax legislation. If the Company cannot establish a valid legal, business or other reason for retaining personal data, it should be securely deleted. The Company specifies the periods for which personal data are stored in Annex A - the Annual Data Audit. After the storage period has expired as stated in Annex A, column (d), personal data should be deleted.

Note that the Company may store some categories of personal data for longer periods where such processing is solely for archiving purposes in the public interest, or historical research purposes. In such cases, the Company must implement appropriate safeguards, such as allowing data subjects to request deletion of some of their personal data.

f. **Integrity and confidentiality**

Personal data must be processed in a manner that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The Company should take appropriate measures that are proportionate to the risk associated with the personal data it holds. Such measures may be technical, such as encryption and password protection of electronic devices and electronic storage media (e.g. USB drives), or organisational, for example, by operating a layered access policy, appropriate vetting of staff who have access to personal data, conducting appropriate due diligence on any third parties that process personal data on the Company's behalf, and binding them by an appropriate engagement contract. The Company regularly reviews and tests its security measures via the DPO and TELA (our Business Mobile IT provider).

g. **Accountability**

Controllers are responsible for compliance with the principles explained above and must be able to demonstrate compliance.

The Company must be in a position of being able to provide evidence of compliance, for example, by way of a data protection policy, documented data protection reviews and a record of data protection training.

8. **Data Subjects' Rights**

Data Protection Legislation confers a number of rights upon data subjects, which controllers must observe. Data subjects' rights are a cornerstone of The Data Protection Legislation and must be dealt with promptly should one arise. The Company is unlikely to receive data subject requests on a regular basis so this Policy does not go into detail, but the Company must be able to recognise a request from a data subject to exercise his or her rights, should one arise. The most relevant of these rights, from the Company's perspective, are summarised below:

a. **Data subject access requests**

Data subjects are entitled to access their personal data held by the Company on request (Article 15 GDPR). The response to a data subject access request must include certain information, such as: the purposes of the processing; the recipients (or categories of recipient) to whom the personal data have or will be disclosed; and individuals' rights to have their data corrected, deleted or to restrict the processing of their data.

Note that under the GDPR, the information must be provided to data subjects free of charge and within one month of the request.

b. **The right to be forgotten**

Data subjects have the right to request the Company erase all data held in respect of them in various circumstances (Article 17 GDPR). However, the right to be forgotten is not an absolute right, and the Company is only obliged to give effect to a request in a number of specific situations, the most relevant of which are likely to be:

(1). Where the purpose for which the personal data were processed no longer applies; or

(2). Where the Company's processing of the personal data is based on consent and the data subject withdraws his or her consent.

c. **The right to rectification**

Data subjects have the right to have incorrect personal data about them corrected without undue delay (Article 16 GDPR).

The Company must endeavour to ensure that any personal data it processes is up to date and correct. Where an error or inaccuracy is discovered, the Company should correct this as soon as possible.

d. **The right to data portability**

Data subjects have the right, in certain circumstances, to access their data in machine-readable format and, where technically possible, to have their data transferred directly from the Company to another data controller (Article 20 GDPR). However, the circumstances in which the right to data portability arises are limited and, at present, seem unlikely to be relevant to the Company.

e. **The right to object**

Data subjects have the right, in a number of specific circumstances, to object to having their personal data processed (Article 21 GDPR). The most relevant of these circumstances are where the processing is based on the Company's legitimate interests. Data subjects may also object to their personal data being processed by the Company for direct marketing purposes.

9. **Our Commitment and Additional Requirements**

a. The Company is committed to transparent, lawful, and fair proportionate processing of personal data. This includes all personal data we process about customers, staff or those who work or interact with us.

b. **Information Asset Owners**

We assign an Information Asset Owner (IAO) to each information asset throughout the organisation, who together with staff with information management responsibilities aid the Company in managing personal data and its associated risks. Our IAOs have joint access to Priava (becoming Momentus) and Salesforce and are aware of their data protection responsibilities.

c. **Privacy Notices**

We publish a Cookie Policy and this Data Protection Policy on our website and provide timely amendments where this is required. We track and make available any changes in these policies. We provide staff with confidentiality and data protection direction in the Staff Handbook and their Fixed Term Contract of Employment.

d. **Training**

We require staff to undertake training on information governance and security which they re-take every year. In addition, specific staff (the DPO) attend complete detailed data protection training modules from the ICO training package.

e. **Breach Notification**

We consider personal data breach incidents and have a reporting mechanism during the weekly staff meeting that is communicated to all staff. We assess whether we need to report breaches to the ICO as the Regulator of DPA without undue delay and where feasible, within 72hrs of the breach. We take appropriate action to report breaches to individual data subjects if required.

f. **Information Rights**

We have a process via the DPO to handle subject access requests and other information rights requests.

g. **Data Protection by Design and Default**

We have considered a procedure to assess processing of personal data perceived to be high risk, that needs a Data Protection Impact Assessment (DPIA) carried out, and The Company does not believe that the nature of its processing is such that there is likely to be a high risk to the rights and freedoms of the data subjects whose personal data it holds. As a result, the Company does not believe that it is necessary for it to undertake any DPIAs. The Company will keep this conclusion under review, including any guidance issued from ICO, or practice in other similar schemes.

h. **Records of Processing Activities (ROPAs)**

We do not routinely process information on law enforcement or special category data, so we do not record such processing activity.

i. **Policies and Procedures**

We produce policies and guidance on information management and compliance that we communicate to staff.

j. **Communications**

We have a clear communication plan and weekly meeting which seeks to embed a culture of privacy and risk orientation.

k. **Contracts**

Our Finance, Charity, Education, Events and Catering staff oversee that our contracts are compliant with UK GDPR.

10. **Roles and Responsibilities**

a. We have an established Information Risk Management process that ensures the risk to personal data across the Company is identified during the weekly staff meeting and appropriately managed. This network's detailed roles and responsibilities comprises of the below.

b. **Data Protection Officer (DPO)**

The Company Data Protection Officer (DPO) is primarily responsible for advising on and assessing our compliance with the DPA and UK GDPR and making recommendations to improve compliance. The Grocers' Company DPO is Eddie Walsh, and he can be contacted at eddie@grocershall.co.uk.

c. **Senior Information Risk Owner (SIRO)**

The SIRO owns the overall risk arising from the processing personal data by the Grocers' Company. Our SIRO is the Clerk - Brigadier Greville Bibby CBE who reports to the Court of Wardens.

11. **Other roles**.

Specific roles are assigned throughout our Company hierarchy to manage personal data we process and the associated risks in terms of responsibilities, decision making and monitoring compliance.

a. **Information Asset Owners (IAOs)**

IAOs have local responsibility for data protection compliance in their area/directorate.

b. **Information Asset Managers (IAMs)**

IAMs support IAOs in complying with their duties regarding the processing of personal data.

c. Specific personnel are responsible for issuing, reviewing and communicating corporate information management policies and procedures. The DPO advises on compliance with data protection and ensures IT solutions have a privacy by design approach.

12. **Monitoring**

Compliance with this policy will be monitored via the DPO and the responsible staff reporting to the SIRO and Court of Wardens.

13. **Feedback on this document**

If you have any feedback on this document, please contact the DPO, Eddie Walsh, eddie@grocershall.co.uk.

14. **Version History**

Version	Changes made	Date	Made by
0.1	Document created	08/01/2025	Eddie Walsh
2.0	First draft release	22/01/2025	Eddie Walsh
3.0	Various amendments	26/02/2025	Eddie Walsh

Annex:

A – The Worshipful Company of Grocers Data Audit dated 22-Jan-2025.