



For the purposes of the General Data Protection Regulation ("GDPR") and UK data protection laws, the Data Controller is Ainsdale Lunch and Leisure whose Registered Office is at, Ainsdale Methodist Church, Liverpool Road, Ainsdale, Southport, PR8 3NQ.

1 Introduction and Scope

Ainsdale Lunch and Leisure (ALL) collects and uses personal data about people with whom it deals in order to operate. This data covers current, past and prospective employees, trustees, volunteers, service users and stakeholders. In addition, it may occasionally be required by law to collect and use personal data to comply with the requirements of government departments, the Charity Commission or Companies House. Any personal information must be dealt with properly however it is collected, recorded and used, whether on paper, in a computer, or recorded in other media.

This policy sets out the principles to which ALL conforms. It relates to all personal data held by ALL, in any form, for which ALL is the Data Controller. It applies to all employees of ALL (whether paid or voluntary) and any other person or external data processor that has access to ALL personal information. Application of these principles by ALL is described in the ALL Privacy Policy.

2 Policy statement

ALL fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 2018 and in the General Data Protection Regulations 2018. ALL will therefore aim to ensure that all employees, trustees, volunteers, contractors, agents, consultants, partners, external agencies or other servants of ALL who have access to any personal data held by or on behalf of ALL, are fully aware of and abide by their duties and responsibilities.

3 Personal data

Personal data is data relating to a living individual who can be identified from that data, or from that data combined with other information that is in the possession of, or is likely to come into the possession of the Data Controller.

Personal data includes an 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.

4 The principles of data protection

The Data Protection Act 2018 stipulates that anyone processing personal data must comply with Six Principles of good practice. These Principles are legally enforceable and require that personal information is:

1. used fairly, lawfully and transparently
2. used for specified, explicit purposes
3. used in a way that is adequate, relevant and limited to only what is necessary
4. accurate and, where necessary, kept up to date
5. kept for no longer than is necessary



6. handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, biometrics (where used for identification), health and sex life or orientation.

The data subject also has the following rights under the act:

- to be informed about how their personal data is being used;
- to access personal data;
- to have incorrect data updated;
- to have data erased;
- to stop or restrict the processing of their personal data;
- data portability (allowing them to get and reuse their data for different services);
- to object to how their data is processed in certain circumstances.

They also have rights when personal data is used by an organisation for:

- automated decision-making processes (without human involvement);
- profiling, for example to predict behaviour or interests.

5 Conditions for processing data

Personal data may only be processed when at least one of the following conditions is met:

- The individual whom the personal data is about has given clear consent to the processing for a specific purpose.
- The processing is necessary in relation to a contract which the individual has entered into; or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions
- The processing is in accordance with the "legitimate interests" condition.

6 Roles and responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

The ALL General Manager has primary responsibility to ensure compliance with the principles of the Data Protection Act whenever personal data is processed within ALL. The ALL General Manager will ensure that any staff or volunteers who have access to personal data are aware of



the principles of the Data Protection Act and of the procedures adopted within ALL in order to comply with the Act. The ALL General Manager will also receive and action requests for access to individual's personal data.

ALL Trustees will provide support and approval for this Data Protection Policy and any related initiatives across ALL. They will address any Data Protection related issues that arise and generate initiatives or communications as necessary to ensure compliance with this policy.

7 Ensuring compliance

In order to meet its obligations under the Data Protection Act, ALL will:

1. **Tell people what ALL is doing with their data**
2. **Adequately train or supervise staff and volunteers**
Familiarity with the Data Protection and Privacy Policies will be included in staff and volunteer induction.
3. **Protect personal data on computer with strong passwords**
Personal data must only be held on computers secured with strong passwords.
4. **Ensure all portable devices are securely stored**
All portable devices – such as memory sticks and laptops – used to store personal information must be kept in locked storage when not in use.
5. **Only keep people's information for as long as necessary**
Retention periods for each type of Personal Data stored are given in the following section along with the arrangements for its secure deletion/destruction once it is no longer required.

8 Actual data held

8.1 Employees

Each employee has a personnel file. This is held in a locked drawer in the office with access limited to the ALL General Manager. Employee records are not currently held electronically. Employees have a right to look at their own file on application to the ALL General Manager. Records of payments to employees are held for 7 years as required by Inland Revenue and then destroyed by shredding or deleting if held online. Files of former employees will be held securely in a locked drawer in the office for a period of up to 7 years after which they will be destroyed by shredding. Employees are informed of the storage of their data by the ALL General Manager or, in the case of the General Manager, by a Trustee.

8.2 Volunteers

Each volunteer completes an application form that includes a notification that their data will be stored for ALL administrative purposes and this along with references is stored securely in a locked filing cabinet in the office, it is also held electronically. Access to volunteer data is limited to the ALL General Manager, the Office Manager and the Catering Manager. On a



volunteer ceasing to work for ALL their record will be retained for 2 years after which it will be destroyed by shredding and deleting.

8.3 Service Users

Each member of the Luncheon Club completes an application form which is checked annually by the ALL General Manager or Office Manager. The form includes a notification that the data will be stored for ALL administrative purposes and these are held alphabetically in a ring binder which is stored in a locked filing cabinet and retained for up to 2 years.

Personal information about housebound Service Users is also given to volunteer drivers with the meal they are taking out. On return, the slips are handed back to the ALL office staff and retained for 1 week and then shredded. Records of meals delivered and the drivers concerned are held on computer for up to 2 years and then deleted.

8.4 Stakeholders

Each stakeholder completes an application form. These are held securely in a locked filing cabinet accessible by Trustees only. Records are also held electronically so that the register of members can be easily updated. The application form seeks consent for data to be held.

9 Contact and Complaints

If you have any queries about this privacy policy or how we process your personal data, or if you wish to exercise any of your legal rights, you may contact the ALL General Manager, Helen Stanbury:

- by email: gm@ainsdalelunchandleisure.org.uk;
- by telephone: 01704 574838;
- or by post: ALL, Ainsdale Methodist Church, Liverpool Road, Ainsdale, Southport, PR8 3NQ.

If you are not satisfied with how we are processing your personal data, you can make a complaint to the Information Commissioner. You can find out more about your rights under applicable data protection laws from the Information Commissioner's Office website: www.ico.org.uk.

Policy Reviewed by Board: March 2025

Next Review: March 2026