

CLASP

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

1. Introduction

CLASP needs to gather and use certain information about individuals who are members of the organisation and/or who participate in services run by CLASP.

This policy describes how this personal data must be collected, handled and stored to comply with current data protection legislation and to meet CLASP's standards.

2. Why this policy exists

This data protection policy ensures that CLASP:

- Complies with data protection legislation and follows good practice;
- Protects the rights of its members and service users;
- Is open about how it stores and processes individuals' data;
- Protects itself from the risks of a data breach

3. Data protection legislation

3.1 The General Data Protection Regulations (GDPR) 2018 describe how organisations must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or other materials. There must be a lawful basis for processing personal information. CLASP collects personal data that is necessary for the purposes of its legitimate interests as a charity.

3.2 To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access

- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision-making and profiling

3.3 The GDPR is underpinned by six important principles. These say that personal data must:

1. Be processed fairly and lawfully and in a transparent manner in relation to individuals;
2. Be obtained only for specific, explicit and legitimate purposes;
3. Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Be accurate and kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay;
5. Not held for any longer than necessary;
6. 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.

3.4 Special category data includes information about race, ethnic origin, politics, religion, genetics, health, biometrics, sexual orientation. This is categorised as more sensitive information and, if collected, needs more protection. It puts individuals at risk of discrimination so there must be an additional lawful basis and conditions for processing this information. CLASP does not keep this data except for GP name and surgery and any allergies, food intolerances etc. for use in an emergency or in its day-to-day operations.

- 3.5 Criminal offence data – to process personal data about criminal convictions or offences, there must be a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10. CLASP does not collect this information.

4. People, risks and responsibilities

4.1 Scope

This policy applies to CLASP, any officer of CLASP, all trustees, management committee members and event organisers. It applies to all data that CLASP holds relating to individuals and can include members' names, dates of birth, addresses, telephone numbers and email addresses. We also hold next-of-kin/carer, doctor's name and surgery for use in an emergency and allergies/food intolerances etc. of those attending the Senior Lunch Club. Data on Disclosure and Barring Service (DBS) checks, done with the member's knowledge and permission, are also held.

4.2 Data protection risks

This policy helps to protect CLASP from some very real data risks including:

- Breaches of confidentiality, e.g. information being given out inappropriately;
- Failing to offer choice, e.g. all individuals should be free to choose how CLASP uses data relating to them.

4.3 Responsibilities

Under the GDPR CLASP does not have a statutory requirement to have a Data Protection Officer. Each individual who handles personal data for CLASP has responsibility for ensuring that data is collected, stored and handled appropriately.

However, the following people have key areas of responsibility:

- The Chairman must ensure that CLASP is compliant with GDPR by keeping the Management Committee updated about data protection responsibilities, risks and issues.

- The Secretary must ensure that all membership records held in paper format must be stored safely in a way that complies with GDPR.

4.4 General guidelines

- GDPR policy and all procedures to be reviewed annually by the Management Committee;
- Ensure that everyone who has access to personal data has understands their responsibilities under GDPR.
- Data held on personal devices should be password protected. Strong passwords must be used and not shared. Devices to be protected by approved security software.
- Ensure that all passwords for electronic storage are changed at least annually. This should be completed immediately when CLASP Officers change.
- The only people able to access data covered by this policy should be those who need it for the legitimate running of CLASP and its events. Data should not be disclosed to unauthorised people either within CLASP or externally.
- Personal data should not be shared informally with anyone except with the express consent of the person to whom the data relates.
- Data should be regularly reviewed and updated. If it is found to be out of date or if it is no longer required, it should be deleted or shredded.
- Paper records must be kept securely and not available where unauthorised access might occur.
- Appropriate training to be provided as necessary.

5. Subject access requests

All individuals who are the subject of personal data held by CLASP have the right to:

- Confirmation that CLASP is processing their personal data and for what purpose;
- A copy of their personal data;
- The categories of personal data concerned;
- The retention period for storing personal data or, where this is not possible, the criteria for determining how long it will be stored;
- The existence of their right to request rectification, erasure or restriction or to object to such processing;
- The right to lodge a complaint with the Information Commissioner's Office;
- Information about the source of the data where it was not obtained directly from the individual.

If any individual contacts CLASP requesting this information this is called a "subject access request". Subject access requests should be made in writing or by email to the Chairman.

Proof of identity may be required before releasing the information; once identity has been verified, the information CLASP holds will be provided within 30 days, free of charge. However, requests excessive in nature or repetitive requests may be subject to a fee.

6. Data breach

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access, to personal data. A breach can include:

- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a Trustee or member of the Management Committee;
- Sending personal data to the incorrect recipient;

- Computing devices containing personal data being lost or stolen;
- Alteration of personal data without permission;
- Loss of availability of personal data, e.g. by corruption and accidental loss or destruction.

All data breaches must be reported to the Chairman and a record kept, regardless of whether or not they need to be reported to the Information Commissioner's Office. The Chairman will be responsible for recording such breaches and discerning whether the breach needs to be reported to the ICO.

Certain types of personal data breach must be reported to the ICO within 72 hours of becoming aware of a breach, where feasible. If the breach has a high risk of adversely affecting an individual's rights and freedoms then the individual(s) in question must be notified.

CLASP's insurance provider may also need to be informed to ensure that it is adequately protected in the event of a claim being made against it or it being fined by the ICO.

There are significant fines for failing to notify a breach when required, so all data breaches, no matter how small, should be reported to the Chairman.

7. Providing information

CLASP aims to ensure that individuals are aware that their data is being processed and that they understand:

- How the data is being used, and;
- How to exercise their rights.

To these ends, CLASP has a privacy notice, setting out how data relating to individuals is used.

CLASP's Privacy Notice is available on request from the Secretary (secretary@clasp-clare.co.uk) or on the CLASP website (clasp-clare.co.uk).

8. Review

This policy will be reviewed by CLASP Management Committee annually and ratified by the Board of Trustees.

Approved by the CLASP Management Committee: 14 August 2025

Approved by the Board of Trustees: 10 September 2025