



Chalfont St Peter
Community Centre

Chalfont St Peter Community Centre (CSPCC)

Data Protection Policy

1.The Policy.

This policy applies to all employees, trustees, and volunteers of Chalfont St Peter Community Centre (CSPCC).

CSPCC is committed to protecting the rights and privacy of individuals. We need to collect and use certain types of personal data in order to manage the Centre effectively, including hirings, finances, and administration. All personal data must be collected, stored, and handled securely and in accordance with the law.

This policy is based on the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

2.Purpose and Coverage

This policy covers all personal data processed by CSPCC, whether held electronically or in paper form, including emails, minutes, forms, photographs, and records stored on computers, laptops, or mobile devices.

3.Definitions.

Data Controller

CSPCC (acting through its trustees) is the Data Controller. It determines how and why personal data is processed.

Personal Data

Any information relating to a living individual who can be identified from that data (e.g. names, addresses, telephone numbers, email addresses).

Processing

Any activity involving personal data, including collecting, storing, using, sharing, or deleting it.

Special Category Data

More sensitive personal data such as health information, racial or ethnic origin, religious beliefs, or criminal records.

Data Subject

The individual whose personal data is held or processed.

UK GDPR / Data Protection Act 2018

The legislation governing the use and protection of personal data.



Chalfont St Peter Community Centre

4.Principles

CSPCC will comply with the UK GDPR principles. Personal data must be:

- Processed lawfully, fairly, and transparently
- Collected for specified and legitimate purposes only
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date where necessary
- Kept only for as long as necessary
- Processed in line with individuals' rights
- Kept secure using appropriate technical and organisational measures
- Not transferred outside the UK unless adequate protection is in place

5.How we use Personal Data

We collect personal data only for the purposes of managing CSPCC, including:

- Managing bookings and hirings
- Financial administration
- Communication with users, hirers, trustees, staff, and volunteers

Data will not be used for any other purpose unless legally required or with consent.

6. Individual Rights.

Individuals have the right to:

- Be informed about how their data is used
- Access their personal data
- Request correction of inaccurate data
- Request deletion of data (where applicable)
- Object to or restrict processing in certain circumstances

7.Subject Access Requests (SARs)

Individuals may request access to their personal data. CSPCC will respond within one month.

We may request reasonable proof of identity before releasing information.



8.Responsibilities.

CSPCC trustees are responsible for ensuring compliance with this policy and for overseeing data protection practices.

They will ensure:

- Personal data is handled lawfully and securely
- Staff and volunteers understand their responsibilities
- Appropriate training and guidance are provided where needed
- Data protection procedures are followed consistently

All trustees, staff, and volunteers must:

- Always follow this policy
- Only access personal data when necessary for their role
- Keep information secure and confidential

9.Data Security.

CSPCC will take appropriate steps to protect personal data from:

- Loss
- Misuse
- Unauthorised access
- Disclosure

Security measures include:

- Password protection on devices
- Restricted access to personal data
- Secure storage of paper records
- Careful handling of emails and electronic records

10.Email, Phone and Devices.

- Emails containing personal data should only be stored when necessary and deleted when no longer required
- Personal data should not be shared by phone unless identity is confirmed
- Devices must be password protected and secured when unattended
- Portable devices should be kept secure during travel



11.Data Retention.

Personal data will only be kept for as long as necessary.

Typical retention periods:

- Financial records: up to 7 years
- Employee records: retained as required for legal and operational purposes
- Other records: deleted when no longer needed

12.Data Sharing.

Data may be shared with third parties only where necessary, including:

- Local authorities
- Funding bodies
- Legal or regulatory authorities

Data will only be shared where legally permitted or with consent.

13.Breaches.

Any suspected data breach must be reported immediately to the trustees. Appropriate action will be taken to contain and assess any breach in line with legal requirements.

14.Risk Management.

Failure to handle data properly may result in harm to individuals, legal liability, and reputational damage to CSPCC. All individuals handling data must take their responsibilities seriously.

15. Policy Review.

This policy will be reviewed annually or sooner if required due to changes in legislation or operational needs.