Oughtrington Community Centre
Data Protection Policy

Oughtrington Community Centre
1 Oughtrington Crescent
Lymm
WA13 9JD

Tel. 01925 75 4178
Email contact@oughtrington.co.uk
Website www.oughtrington.co.uk

Charity number 1112982 Company number 05626686

oughtrington community centre
FOR YOU, BY YOU

1. Document control and review history

Version	Date	Description	Editor
0.1	31/03/2024	Initial draft	AO

2. Terms and abbreviations

Term	Description
EU	European Union
GDPR	The General Data Protection Regulation 2018, implemented in the UK via the Data Protection Act 2018
ICO	(UK) Information Commissioners Office, e.g. the UK Supervisory Authority as stated in the GDPR
OCC	Oughtrington Community Centre
“Users of the Centre”	All users of OCC, hirers, volunteers and visitors
UK	United Kingdom

3. Policy Statement

Oughtrington Community Centre (OCC) will take all reasonable and practical steps to manage the Data and Personal Information that we hold and process relating to our Members, Customers and people who have contact with us.

4. About Oughtrington Community Centre (OCC)

Oughtrington Community Centre is a registered Charity and Limited Company, Charity number 1112982 - Company number 05626686, and is comprised of unpaid Trustees, volunteers and members.
Details of the OCC organisation are available on our website and are available in paper format by request.

The postal address for Oughtrington Community Centre is:
Oughtrington Community Centre, 1 Oughtrington Crescent, Lymm, WA13 9JD
The email address for Oughtrington Community Centre is:
Contact@oughtrington.co.uk

The contact phone number for Oughtrington Community Centre is:
01925 75 4178

The website for Oughtrington Community Centre is:
www.oughtrington.co.uk

5. Data Protection Policy

Oughtrington Community Centre needs to collect and use certain types of personal information about the customers and volunteers that we come into contact with, in order to deliver our core services. This personal information must be collected and dealt with appropriately, whether it is stored on paper, in a computer or recorded on other material – and there are safeguards to ensure this under the General Data Protection Regulation 2018 (GDPR).

The following list below of definitions of the technical terms we have used is intended to aid understanding of this policy.

Data Controller – The person who (either alone or with others) decides what personal information OCC will hold and how it will be held or used.

General Data Protection Regulation (GDPR) – The EU/UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that it follows its data protection policy and complies with the GDPR.

Data Subject/Service User – The individual whose personal information is being held or processed by OCC (for example: a customer or hirer, a volunteer, or a member)

'Explicit' consent – is a freely given, specific and informed agreement by a Data Subject* to the processing* of personal information* about her/him. Explicit consent is needed for processing some data as outlined in this policy, including sensitive* data. * See definition

Notification – Notifying the Information Commissioner about the data processing activities of OCC as certain activities may be exempt from notification.

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the GDPR.

Processing – means collecting, amending, handling, storing or disclosing personal information**.**

Personal Information – Information about living individuals that enables them to be identified – e.g. name and address. It does not apply to information about organisations, companies and agencies but applies to named persons, such as individuals, volunteers or employees.

Sensitive data – this refers to data beyond basic personal information and includes

- Racial or ethnic origin
- Political opinions
- Religious or similar beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Criminal record
- Criminal proceedings relating to a data subject's offences

6. Data Controller

The OCC Board of Trustees is the Data Controller under the Act, which means that it determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for. The Secretary of OCC will act on behalf of the Board of Trustees as the Data Controller.

7. Disclosure of Personal Information

OCC may share data with other agencies such as the local authority, funding bodies and other voluntary agencies for reporting and monitoring purposes.
The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows OCC to disclose data (including sensitive data) without the data subject's consent.
These are:

1. Carrying out a legal duty or as authorised by the Secretary of State.
2. Protecting vital interests of a Data Subject or other person.
3. The Data Subject has already made the information public.
4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights.
5. Monitoring for equal opportunities purposes – i.e. race, disability or religion.
6. Providing a confidential service where the Data Subject's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Data Subjects to provide consent signatures.

OCC regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

OCC intends to ensure that personal information is treated lawfully and correctly.
To this end, OCC will adhere to the 8 Principles of Data Protection, as detailed in the GDPR.
Specifically, the Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular shall not be processed unless specific conditions are met,
2. Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes,
3. Shall be adequate, relevant and not excessive in relation to those purpose(s)
4. Shall be accurate and, where necessary, kept up to date,
5. Shall not be kept for longer than is necessary.
6. Shall be processed in accordance with the rights of data subjects under the Act.
7. Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information,

8. Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal information.

OCC will, through appropriate management, strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information,
- Meet its legal obligations to specify the purposes for which information is used,
- Collect and process appropriate information, and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
- Ensure the quality of information used,
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
    - The right to be informed that processing is being undertaken,
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information
    - Take appropriate technical and organisational security measures to safeguard personal information,
- Ensure that personal information is not transferred abroad without suitable safeguards,
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information,
- Set out clear procedures for responding to requests for information.

8. Data collection

OCC is obligated to state a valid lawful basis for data collection and processing. Under GDPR there are 6 lawful bases which include:

- Informed consent
- Contractual
- Legal obligation
- Vital interest
- Public task
- Legitimate interest

OCC has highlighted 'informed consent' as one of the lawful bases of processing data. This is based on the communications we distribute via bulk mailings, both to members of the public who would like to receive information about our services, and to our members.
OCC will only send bulk mailings to those who have given us their informed consent to do so. More information is given below.

OCC has also highlighted 'Contractual' as the second lawful basis of processing data, where we hire or provide facilities on a commercial basis. Given the requirements of OCC to

provide safe facilities to all of our users and to maintain hire records, we consider users who we do not charge a hire fee too (e.g. Luncheon Club) as falling under this lawful basis for processing data.

OCC has also highlighted 'legitimate interest' as the third lawful basis of processing data. This is due to the fact that OCC cannot conduct core business activities without collecting information about the various third sector organisations based in the local area, including contact details. In cases where organisations are entirely volunteer led, this could result in personal information being linked to an organisation. OCC will endeavour to explain the terms of legitimate interest in relation to organisational information to stakeholders.

9. Informed consent

Informed consent is when a Data Subject clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data and then gives their consent.
OCC will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.
When collecting data, OCC will ensure that the Data Subject:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Data Subject decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
- Has received sufficient information on why their data is needed and how it will be used

10. Data Storage

Information and records relating to stakeholders and clients will be stored securely using a secure online cloud-based system which receives regular software updates and will only be accessible to authorised Trustees / staff and volunteers who have received appropriate training.
Information will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

It is OCC's responsibility to ensure all personal and company data is non-recoverable from any computer hardware previously used within the organisation, which has been passed on/sold to a third party / disposed of.

OCC will ensure that all personal data is protected by encrypted and/or password protected systems.

11. Data access and accuracy

All Data Subjects have the right to access the information that OCC holds about them. Upon a data access request, OCC will first establish the true identity of the subject, and endeavour to release all data relating to that subject within 5 working days at no cost to the individual. Individuals have the right to expect organisations to keep accurate data about them. OCC will take all reasonable steps to ensure that this information is kept up to date by contacting data subjects every 12 months to establish whether there have been any changes.

Individuals also have the right to erasure, except in cases where there is a lawful reason where data needs to be retained. OCC will action erasure requests within 5 working days. Where erasure is not possible, OCC will anonymise data as fully as possible, to the satisfaction of the data subject.
This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the General Data Protection Regulation 2018.

Individuals have the right to complain to the UK Data Protection Supervisory Authority, the Information Commissioner's Office (ICO), via their website: https://ico.org.uk/global/contact-us/ or phone line (0303 123 1113 Monday to Friday, 9am to 5pm)

12. Notification of a Personal Data Breach

A personal data breach (PDB) can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data:

> *e.g. under an OCC assessment, is there likely to be a high risk to individuals' rights and freedoms?. If so, then under the GDPR, the data Controller (e.g. OCC) must notify the affected users and the relevant supervisory authority "without undue delay and, where feasible not later than 72 hours after having become aware of it…"*

The 72 hour period includes weekends and public holidays; timely notification is important.

The UK Supervisory Authority is the Information Commissioners Office (ICO).
The ICO has a tool on their website to assist with determining actions required in the event of a data breach: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ (this includes a link to report a data breach online).
The ICO helpline is 0303 123 1113