

1.0 Scope

1.1 This policy applies to;

- all staff employed by 3CS (paid or unpaid) or
- is otherwise required by 3CS to **gather, store** or **process** personal data on behalf of 3CS or
- customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

2.0 Legal Provisions

2.1 The principles of General Data Protection Regulation¹ (EU Regulation 2016/679) provides the legal direction to 3CS to safeguard 'personal data'.

2.2 3CS acknowledge the right to privacy² by recognising the need to take steps to ensure individuals have sufficient control over their information. 3CS recognise it is important to remember that data protection isn't just about digital information but all personal information, including that which is recorded or stored in paper copies.

3.0 Personal Data

3.1 This is **any information** which relates directly to an individual and can be linked directly to them. For example; name, phone number, email address, photographs, customer reviews, genetic and economic data.

3.2 This kind of data is the focus of GDPR and data protection. 3CS recognise the requirements of pseudonymous data within this policy and will consider it as personal data.

3.3 Data subject

A data subject is someone who can be identified from personal data. The data could be their name, address, telephone number or something else – but if it's about a person, then they're the data subject. They are the 'subject' of the data.

In general terms, 'data subjects' at 3CS will mean its customers, employees, volunteers and service users. 3CS recognise that anyone else whose personal data it uses will be a data subject, too.

4.0 3CS – Data Protection Values

4.1 The default position of 3CS is to always respect the privacy of the individual and not presume 3CS has the consent to use personal data.

4.2 3CS will endeavour to ensure it legally complies with the following:

- How 3CS **gather** information, in particular how 3CS evidence 'consent'
- How securely 3CS **store** information in particular 'special categories'³

¹ Referred to throughout as "GDPR" the EU's agreed standards for data protection that are also written into UK law through the Data Protection Act 2018 (DPA 2018).

² Article 9 of the European Convention on Human Rights

³ They can be processed only with explicit consent to do so, or if it is a necessity in performing a contract. This type of information can, however, be gathered in an anonymised form for the purpose of research and monitoring.

- Racial and ethnic origin
- Political opinions

- How 3CS **comply with reasonable requests** for the information it holds
- How 3CS can **evidence** any of the above in the event of an audit
- Ensuring that 3CS has useable, robust, transparent and legally defensible **policies** and acceptable **processes** in place .

5.0 3CS – Data Protection Standards

5.1 At every step of processing data, 3CS will consider:

- Should we be collecting this?
- Is this useful and accurate?
- Have we got clear permission or valid justification to use this?
- Should we still be holding this?
- Is our data held securely and safely?
- Is this request genuinely from the individual concerned?
- Are the businesses we work with also compliant?

5.2 The GDPR defines six principles for processing of personal data. It is these six principles that provide the underpinning data protection standards for which 3CS will endeavour to comply.

5.3 These are:

1. Lawfulness, fairness and transparency

3CS will ensure data should be gathered and used in a way that is **legal, fair and understandable**. Our members and the general public have the right to know what is being gathered and have this corrected or removed.

2. Purpose limitation

3CS will only use data for a **legitimate purpose** specified at the time of collection. This data should not be shared with third parties without permission.

3. Data minimisation

The data collected by 3CS should be limited only to what is required for the purpose stated. 3CS should not collect data en masse without purpose.

4. Accuracy

The personal data held by 3CS should be **accurate**, kept up to date, and, if it is no longer accurate, should be rectified or erased.

5. Storage limitation

Personal data should only be **stored for as long as is necessary**. Data can be archived securely and used for research purposes in the future. Where possible, the personally identifiable information should be removed to leave anonymous data.

-
- Religious or philosophical beliefs
 - Trade Union membership
 - Data on health, sex life or sexual orientation
 - Genetic or biometric data

6. Integrity and confidentiality

Personal data should be held in a **safe and secure way** that takes reasonable steps to ensure the security of this information and avoid accidental loss, misuse or destruction.

6.0 Compliance

Data Protection Manager

6.1 This role is *not* a Data Protection Officer (DPO) or Data Controller or Data Processor as defined under the Act. But it follows parallel aims to ensure that the interests of 3CS are compliant with the DPA and the GDPR processes relating to the personal data of its staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection rules.

6.2 The Data Protection Manager will:

- **Monitor** 3CS data protection compliance;
- **Inform** and **assist** 3CS of its data protection obligations;
- Act as a **contact point** for data subjects and the relevant supervisory authority – the ICO (Information Commissioner’s Office).

6.3 There are **six valid reasons for storing and using personal information known as ‘conditions for processing’**.

6.4 Much of the management of 3CS - such as administering membership and other activities people would reasonably expect, could be classed as **‘legitimate interests’** but other communications, outside of the core activities of 3CS may rely on **‘consent’**.

6.5 When using ‘legitimate interests’, 3CS should ensure this meets **three simple checks**:

1. 3CS should be able to identify a sound, **justifiable** interest for 3CS
2. 3CS can prove that processing is **necessary** to achieve this, and
3. 3CS should balance this interest against the **rights of the individual(s)**.

6.6 Processing

6.7 Processing means taking any action with someone’s personal data. This begins when the Data Protection Manager starts making a record of information about someone, and continues until the information is no longer needed and it’s been securely destroyed.

6.8 If 3CS hold information on someone, 3CS recognise it counts as processing even if 3CS don’t do anything else with it.

6.9 Other types of data processing include actions such as organising and restructuring the way 3CS saves the data and making changes to it eg updating someone’s address or record, and sharing it or passing it on to others.

7.0 Rights and requests

7.1 Individuals have several rights under GDPR which 3CS will adhere to. These generally allow them to ask 3CS to do something, or stop doing something, with their personal data.

7.2 3CS recognise the eight individual rights which 3CS will endeavour to comply with these rights whenever they're used, unless it's an exceptional situation.

7.3 As a small club the three main rights likely to be relevant to 3CS are the right of access, the right to object and the right to be informed:

- The right of access is when someone asks 3CS for a copy of the data 3CS has on them. This is also known as a subject access request - or SAR. 3CS acknowledge it has one month to deal with a SAR.
- The right to object means people can object to specific processing of their personal data. In such circumstances 3CS will stop using their data for certain purposes unless 3CS have a good reason to continue. For example, if a customer objects to 3CS using their details to send them postal marketing, 3CS could suppress or flag their details to prevent further marketing material getting sent again.
- The right to be informed usually means that 3CS have to tell people that 3CS have their data and what the club doing with it.

7.4 This policy also acknowledges the other five rights:

- The right to rectification means people can ask 3CS to correct their data if it isn't accurate.
- The right to erasure is when someone asks 3CS to delete their data. It is also known as the 'right to be forgotten' and means that in certain specific situations, 3CS may have to delete their data upon request. For example, if 3CS collected someone's personal data and it's now no longer valid for the reason the club collected it, they could ask 3CS to delete it.
- The right to restrict processing means that 3CS have to temporarily stop processing someone's data if they ask 3CS to.
- The right to data portability gives people more control over their data where it's held electronically if it's personal data they've supplied themselves. It's intended to make it easy for them to provide it to another data controller if they need to. The data 3CS hold about them electronically has to be made easily accessible and transferable. Also, if requested, 3CS will provide it to them or to another organisation on their behalf. However, this right only applies when the controller is relying on 'consent' or 'performance of a contract', and when they're processing the data by automated means.

7.5 3CS will endeavour to respond to subject access requests within the specified times. 3CS can and should request valid proof of identification from the individual before proceeding with the request.

7.6 If 3CS have shared data with a third party (although unlikely), 3CS may have to notify them of changes or deletion. Similarly, a third party may pass on a request from an individual instructing 3CS to alter or delete shared data.