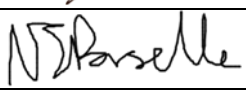
DATA PROTECTION POLICY

	Name	Designation	Date	Signature
Author	Victoria Haley	Administration Officer	21/02/23	
Approvals	Paul Lovell	Data Protection Lead Trustee	27/03/23	
	Norman Parselle	Chief Executive Officer	22/02/23	

Revision	Date	Effect on		Reason for revision and description	Author
		Page	Para		
1.0	July 2016	All	All	First Data Protection Policy	Norman Parselle
2.0	June 2017	All	All	Full Review	Norman Parselle
3.0	June 2018	All	All	Full Review	Dan Harvey
4.0	July 2020	All	All	Full Review	Dan Harvey
5.0	Aug 2021	All	All	Full Review	Dan Harvey
6.0	Aug 2022	All	All	Full Review	Victoria Haley
7.0	Feb 2023	All	All	Data Protection Officer Details	Victoria Haley

1. PURPOSE

This policy establishes an effective, accountable, and transparent framework for ensuring compliance with the requirements of the GDPR.

2. SCOPE

This policy applies to all County in the Community employees responsible for the processing of personal data on behalf of their participants associated with their activities.

3. POLICY STATEMENT

County in the Community is committed to working in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.

This policy sets forth the expected behaviours of County in the Community employees and third parties in relation to the collection, use, retention, transfer, disclosure, and destruction of any personal data belonging to a County in the Community participant (i.e., the data subject).

Personal data is any information (including opinions and intentions) which relates to an identified or identifiable natural person. Personal data is subject to certain legal safeguards and other regulations, which impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. County in the Community as a Data Controller is responsible for ensuring compliance with the data protection requirements outlined in this policy. Non-compliance may expose the CCO to complaints, regulatory action, fines and/or reputational damage.

County in the Community's leadership is fully committed to ensuring continued and effective implementation of this policy and expects all employees and third parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

3.1 Governance

3.1.1 Data Protection Officer

To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, County in the Community has appointed a Data Protection Officer. The Data Protection Officer's duties include:

- Informing and advising County in the Community and its employees who carry out processing pursuant to data protection regulations, national law or European Union based data protection provisions.
- Ensuring the alignment of this policy with data protection regulations, national law or European Union based data protection provisions.
- Acting as a point of contact for and cooperating with Data Protection Authorities (DPAs).
- The establishment and operation of a system providing prompt and appropriate responses to data subject requests.

- Informing the charity's manager and trustees of any potential corporate, civil and criminal penalties which may be levied against County in the Community and/or its employees for violation of applicable data protection laws.

3.1.2 Compliance Audit

To confirm that an adequate level of compliance is being achieved by all County in the Community staff/trustees in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for all such services/entities. Each audit will, as a minimum, assess:

- Compliance with policy in relation to the protection of personal data, including:
- The assignment of responsibilities.
- Training of employees and knowledge of policies and procedures.
- Checking the accuracy and relevance of data held.
- Destroying data which is deemed irrelevant or inaccurate.

3.2 Data Protection Principles

County in the Community has adopted the following principles to govern its collection, use, retention, transfer, disclosure, and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. This means, County in the Community must tell the data subject what processing will occur (transparency), the processing must match the description given to the data subject (fairness), and it must be for one of the purposes specified in the applicable data protection regulation (lawfulness).

Principle 2: Purpose Limitation. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means County in the Community must specify exactly what the personal data collected will be used for and limit the processing of that personal data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation. Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. This means County in the Community must not store any personal data beyond what is strictly required.

Principle 4: Accuracy. Personal data shall be accurate and, kept up to date. This means County in the Community must have in place processes for identifying and addressing out-of-date, incorrect, and redundant personal data.

Principle 5: Storage Limitation. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. This means County in the Community must, wherever possible, store personal data in a way that limits or prevents identification of the data subject.

Principle 6: Integrity & Confidentiality. Personal data shall be 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. County in the Community must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

3.3 Data Collection

3.3.1 Data Sources

Personal data should be collected only from the data subject unless one of the following apply:

- The nature of the business purpose necessitates collection of the personal data from other persons or bodies.
- The collection must be carried out under emergency circumstances in order to protect the vital interests of the data subject or to prevent serious loss or injury to another person.

If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional secrecy obligation
- A national law expressly provides for the collection, processing, or transfer of the personal data.

Where it has been determined that notification to a data subject is required, notification should occur promptly, but in no case later than:

- One calendar month from the first collection or recording of the personal data
- At the time of first communication if used for communication with the data subject
- At the time of disclosure if disclosed to another recipient.

3.3.2 Data Subject Consent

Each County in the Community coach will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, County in the Community is committed to seeking such consent. The Data Protection Officer has established a system for obtaining and documenting data subject consent for the collection and processing of information. Please see 'CitC Data Consent Form'.

3.3.3 Data Subject Notification

Each County in the Community member of staff will, when required by applicable law, contract, or where it considers that it is reasonably appropriate to do so, provide data subjects with information as to the purpose of the processing of their personal data. Please see 'CitC Privacy Notice'. When the data subject is asked to give consent to the processing of personal data and when any personal data is collected from the data subject, all appropriate

disclosures will be made, in a manner that draws attention to them, unless one of the following apply:

- The data subject already has the information.
- A legal exemption applies to the requirements for disclosure and/or consent. The disclosures may be given orally, electronically or in writing. If given orally, the person making the disclosures should use a suitable script or form approved in advance by the Data Protection Officer. The associated receipt or form should be retained, along with a record of the facts, date, content, and method of disclosure.

3.3.4 External Privacy Notices

The County in the Community website will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of applicable law.

3.4 Data Use

3.4.1 Data Processing

County in the Community uses the personal data of its contacts for the following broad purposes:

- The general running and administration of County in the Community.
- To provide, and improve, provision for County in the Community's stakeholders.
- The ongoing administration, monitoring and evaluating of CCO activity.

The use of a contact's information should always be considered from their perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a contact's expectations that their details will be used by County in the Community to let them know about a session coming up, which they have recently been involved in and have been requested to receive updates about. However, it will not be within their reasonable expectations that County in the Community would then provide their details to third parties (e.g., Newport County AFC) for marketing purposes.

County in the Community will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, County in the Community will not process personal data unless at least one of the following requirements are met:

- The data subject has given consent to the processing of their personal data for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person.
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When making a determination as to the compatibility of the new reason for processing, guidance and approval must be obtained from the Data Protection Officer before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, County in the Community's DPO will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected: Any link between the purpose for which the personal data was collected and the reasons for intended further processing.

- The context in which the personal data has been collected, in particular regarding the relationship between data subject and the Data Controller.
- The nature of the personal data, in particular whether special categories of data are being processed, or whether personal data related to criminal convictions and offences are being processed.
- The possible consequences of the intended further processing for the data subject.
- The existence of appropriate safeguards pertaining to further processing, which may include encryption, anonymisation or pseudonymisation.

3.4.2 Special Categories of Data

County in the Community will only process special categories of data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply:

- The processing relates to personal data which has already been made public by the data subject.
- The processing is necessary for the establishment, exercise, or defence of legal claims.
- The processing is specifically authorised or required by law.
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

In any situation where, special categories of data are to be processed, prior approval must be obtained from the Data Protection Officer, and the basis for the processing clearly recorded with the personal data in question. Where special categories of data are being processed, County in the Community will adopt additional protection measures.

Examples of sensitive data could be:

- race
- ethnic origin
- religion
- health

3.4.3 Children's Data

Children under the age of 14 are unable to consent to the processing of personal data for information society services (any service normally provided for payment, by electronic means and at the individual request of a recipient of services). Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility. Please see the 'Data Consent Form' for more information in regard to obtain children's consent from parents/guardians.

3.4.4 Data Quality

Each County in the Community member of staff will adopt all necessary measures to ensure that the personal data it collects, and processes is complete and accurate in the first instance and is updated to reflect the current situation of the data subject. The measures adopted by County in the Community to ensure data quality include:

- Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.
- Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.
- The removal of personal data if in violation of any of the data protection principles or if the personal data is no longer required.
- Restriction, rather than deletion of personal data, in so far as:
    - a law prohibits erasure.
    - erasure would impair legitimate interests of the data subject.
    - the data subject disputes that their personal data is correct, and it cannot be clearly ascertained whether their information is correct or incorrect.

3.5 Data Retention

To ensure fair processing, personal data will not be retained by County in the Community for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed. The length of time for which County in the Community needs to retain personal data is set out in County in the Community's 'Data Retention and Data Breach Policy'. This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data should be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

3.6 Data Protection

Each County in the Community employee will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by virtue of human action or the physical or natural environment. A summary of the personal data related security measures is provided below:

- Prevent unauthorised persons from gaining access to physical personal data collected. To help protect this information, the CCO have introduced the following security measures regarding Data Protection Policy tractions

1. Restricted access to the CCO premises – using intercom to enable entry, visitors required to sign in
2. All hard copies of personal data to be stored in a designated, secure and lockable cupboard area (on the first floor of the building)
3. Each employee will have a lockable storage cabinet, which may be used to store personal data while inputting into our electronic monitoring and evaluation system (short-term), prior to moving it to designated storage area (please see above)
4. Separate meeting and consultation rooms for visitors to the CCO facility, to limit personnel that could potentially encounter personal data held by employees during working hours

- Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.
- Ensure that personal data in the course of electronic transmission during transport cannot be read, copied, modified or removed without authorisation.
- Ensure that in the case where processing is carried out by a Data Processor (member of staff), the data can be processed only in accordance with the instructions of the Data Controller (CITC).
- Ensure that personal data is protected against undesired destruction or loss (stored in the correctly identified facility).
- Ensure that personal data is not kept longer than necessary.

3.7 Data Subject Requests

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights related to:

- Information access.
- Objection to processing.
- Objection to automated decision-making and profiling.
- Restriction of processing.
- Data portability.
- Data rectification.
- Data erasure.

If an individual makes a request relating to any of the rights listed above, County in the Community will consider each such request in accordance with all applicable data protection laws and regulations. No administration fee will be charged for considering and/or complying with such a request unless the request is deemed to be unnecessary or excessive in nature. Once a request has been raised, the County in the Community member of staff will then notify the DPO. Data subjects are then sent a Subject Access Request (SAR) form and are entitled to obtain their information, based upon the DPO's receipt of the completed SAR.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

3.8 Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- The assessment or collection of a tax or duty.
- By the order of a court or by any rule of law.

If any County in the Community member of staff processes personal data for one of these purposes, then it may apply an exception to the processing rules outlined in this policy but only to the extent that not doing so would be likely to prejudice the case in question. If any member of staff or trustee receives a request from a court or any regulatory or law enforcement authority for information relating to a County in the Community contact/participant, you must immediately notify the Data Protection Officer who will provide comprehensive guidance and assistance.

3.9 Data Protection Training

All County in the Community employees that have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training. In addition, County in the Community will provide regular Data Protection training and procedural guidance for their staff, when deemed necessary but annually as a minimum.

3.10 Data Transfers

County in the Community may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection (i.e., third countries), they must be made in compliance with an approved transfer mechanism.

- The data subject has given Consent to the proposed transfer.
- The transfer is necessary for the performance of a contract with the data subject
- The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.
- The transfer is legally required on important public interest grounds.
- The transfer is necessary for the establishment, exercise, or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject

3.11 Data Storage

There are a number of ways in which records can be kept including paper-based format, electronically on a server or computer hard-drive or on a device such as a USB memory stick. In recognition of this range of storage methods County in the Community will adopt the following statements of principle for storage of records:

- Records containing the personal details of staff or project participants will be stored securely either through password protection electronically or through the use of lockable storage for paper-based records.
- That personal records will not be kept on unsecured media, such as a USB memory stick.
- That County in the Community staff will periodically review the records for which they have responsibility and retain or destroy them as appropriate.
- All the above has been recommended by Paul Fry, IT Manager at paul@cip.support (Cardiff).

3.12 Complaints Handling

Data subjects with a complaint about the processing of their personal data, should put forward the matter in writing to the Data Protection Officer. An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case. The Data Protection Officer will inform the data subject of the progress and the outcome of the complaint within a reasonable period. If the issue cannot be resolved through consultation between the data subject and the Data Protection Officer, then the data subject may, at their option, seek redress through mediation, binding arbitration, litigation, or via complaint to the Data Protection Authority within the applicable jurisdiction.

3.13 Breach Reporting

Any individual who suspects that a personal data breach has occurred due to the theft or exposure of personal data must immediately notify the Data Protection Officer providing a description of what occurred. Notification of the incident can be made via e-mail or via phone – as outlined in the 'Data Retention and Data Breach Policy'. The Data Protection Officer will investigate all reported incidents to confirm whether or not a personal data breach has occurred. If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved.

4. ROLES AND RESPONSIBILITIES

4.1 Implementation

The Data Protection Officer, CCO Manager and Trustees must ensure that all County in the Community employees responsible for the processing of personal data are aware of and comply with the contents of this policy. In addition, County in the Community will make sure all third parties engaged to process personal data on their behalf (i.e., payroll, accountants) are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties, whether companies or individuals, prior to granting them access to personal data controlled by County in the Community.

4.2 Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer. (admin@countyinthecommunity.co.uk).

5. REVIEW

This policy will be reviewed by the Data Protection Officer every three years, unless there are any changes to regulations or legislation that would enable a review earlier.

6. RECORDS MANAGEMENT

Staff must maintain all records relevant to administering this policy and procedure in electronic and written form, in a recognised County in the Community record-keeping system, outlined by the DPO.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.

7. TERMS AND DEFINITIONS

General Data Protection Regulation (GDPR): The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU.

Data Controller: the entity that determines the purposes, conditions, and means of the processing of personal data. (CITC)

Data Processor: the entity that processes data on behalf of the Data Controller. (Staff, Views)

Data Protection Authority: national authorities tasked with the protection of data and privacy as well as monitoring and enforcement of the data protection regulations within the Union.

Data Protection Officer (DPO): an expert on data privacy who works independently to ensure that an entity is adhering to the policies and procedures set forth in the GDPR.

Data subject: a natural person whose personal data is processed by a controller or processor.

Personal data: any information related to a natural person or 'data subject', that can be used to directly or indirectly identify the person.

Privacy Impact Assessment: a tool used to identify and reduce the privacy risks of entities by analysing the personal data that are processed and the policies in place to protect the data.

Processing: any operation performed on personal data, whether or not by automated means, including collection, use, recording, etc.

Profiling: any automated processing of personal data intended to evaluate, analyse, or predict data subject behaviour.

Regulation: a binding legislative act that must be applied in its entirety across the Union.

Subject Access Right: also known as the Right to Access, it entitles the data subject to have access to and information about the personal data that a controller has concerning them.

8. DATA RETENTION AND BREACH

Purpose
The purpose of this policy is to specify County in the Community's guidelines for retaining different types of personal data.

Detail
The scope of this policy covers all County in the Community participant's personal data stored on company-owned, company-leased, and otherwise company-provided systems and media, regardless of location. These records may be created, received, or maintained in hard copy or electronically.

Policy Statement
The need to retain personal data varies widely with the type of data collected. Some personal data can be immediately deleted, and some must be retained until reasonable potential for future need no longer exists. This Data Retention and Data Breach Policy provides guidelines to ensure that all applicable regulations and County in the Community's policies on personal data retention are consistently applied throughout the organisation.

Reasons for Data Retention
Some personal data must be retained in order to protect the company's interests, comply with regulatory requirements, preserve evidence, and generally conform to good business practices. Personal data may be retained for one or several of the following reasons:

- Business requirements
- Regulatory requirements
- Possible litigation
- Accident investigation
- Security incident investigation
- Intellectual property preservation

Retention Periods
Different types of data will be retained for different periods of time:

- Participant's personal data: Personal data will be held for as long as the individual is a participant of the CCO.
- Personal employee data: General employee data will be held for the duration of employment and then for 6 years after the last day of contractual employment. Employee contracts will be held for 6 years after last day of contractual employment.
- Personal tax payments will be held for 2 years.
- Records of leave will be held for 6 years.
- Recruitment details: Interview notes of unsuccessful applicants will be held for 6 months after interview. This personal data will then be destroyed.
- Health and Safety: 5 years for records of major accidents and dangerous occurrences.
- Operational data: Most company data will fall in this category. Operational data will be retained for 6 years.
- Critical data including Tax and VAT: Critical data must be retained for 6 years.

Data Duplication
When identifying and classifying participant's personal data, it is important to also understand where that data may be stored, particularly for duplicate copies, so that this policy may be applied to all duplicates of the information.

Data Destruction
When the retention timeframe expires, County in the Community will actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by the Data Protection Officer and County in the Community's senior management team.

The company specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to himself or herself or destroying data in an attempt to cover up a violation of law or company policy is particularly forbidden.

9. STAFF RESPONSIBILITIES

Compliance, monitoring and review
The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to performing daily activities at County in the Community rests with the Data Protection Officer.

All members of staff that deal with collecting and processing personal data are responsible for processing this data in full compliance with the relevant County in the Community policies and procedures.

Reporting in case of a data breach
In the case of possible data breach, the staff member(s) who first identifies the breach or incident, must immediately report all details of the incident to the Data Protection Officer.

The Data Protection Officer is required to report a personal data breach to the competent Data Protection Authority not later than 72 hours after becoming aware of it. The notification must include at least:

- a description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned.
- the name and contact details of the relevant Data Protection Officer or contact point.
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Data Protection Officer must communicate the breach to the data subject(s) without undue delay. The communication must describe in clear and plain language, the nature of the breach and at least:

- the name and contact details of the relevant Data Protection Officer or contact point;
- the likely consequences of the data breach; and
- measures taken or proposed by the controller to address the breach and/or mitigate its effects.

Records Management

Staff must maintain all records in terms of carrying out this policy and procedure in hard copy (paper) and electronic form in the recognised County in the Community Data Protection record-keeping system.

All records relevant to administering this policy and procedure will be maintained for a period of 5 years.