



# East Sussex Community Voice

## Record Keeping and Retention Policy

Version	Date of next review by ESCV Board	Date of adoption by ESCV Board
1	n/a	30 <sup>th</sup> March 2021
2	March 2023	March 2024
3	March 2026	
4		
5		

### 1 Purpose

1.1 This policy identifies the information held by East Sussex Community Voice CIC (ESCV) and clarifies the legal and best practice requirements for information retention and deletion.

1.1 Accurate and proportionate data records are kept by East Sussex Community Voice CIC to:

- comply with all employment, charity and company legal requirements
- comply with quality assurance systems
- provide a high-quality service to clients and the public

1.2 East Sussex Community Voice CIC's has a responsibility to ensure our activities are compliant with the General Data Protection Regulation (2018).

1.3 By listing which information to keep and how long documents must be retained, we are ensuring the appropriate storage, security and disposal of important records and personal information. Employees of ESCV must uphold this policy and follow the guidelines detailed below.

### 2 Scope

2.1 This policy and procedure applies across all entities or subsidiaries owned or controlled by East Sussex Community Voice CIC and to all employees, including part-time, temporary, or contract employees, who handle corporate and personal information.

2.2 This policy covers all electronic and physical records that contain personal information, including:

- Recruitment documents and personnel files
- Finances, accounts and financial records



- Email conversations
- Meeting minutes
- Spreadsheets
- Corporate documents and records
- Presentations
- Any scanned documents submitted by employees or external sources

2.3 Records are retained for the period specified in the retention schedule below, which except for items that must be stored permanently, are then appropriately destroyed.

2.4 Employees who access, contribute to, or manage any documents or information sources related to the records mentioned above must follow these guidelines, and all ESCV staff and Board members should be aware of their obligations around storage and disposal.

### 3 Procedure

3.1 All paper-based records are held securely in locked storage. These may include: contracts, HR records, banking information and financial statements, signed consent forms and project documentation. Wherever possible such records are scanned and saved electronically in a suitable location, with the paper version then securely destroyed.

3.2 Electronic files are kept securely stored on the ESCV SharePoint system, server or on other web-based platforms. These platforms are user restricted and/or password protected.

Platforms may include the website content management system (CMS) [Feedback Centre], Microsoft Teams, and web-based platforms (e.g. SmartSurvey, MailChimp etc) and banking/accounting websites.

3.3 Members of the public who choose to engage with ESCV are made aware where and when their personal information is collected and stored and informed that personal information will be kept confidential and will not be shared unless express consent has been given or there is a legal basis to do so.

When asking for consent to pass on personal details, ESCV staff, Board members, volunteers and representatives will confirm how information will be used and passed on and clarify the rights to amendment and deletion set out under GDPR.

3.4 ESCV will keep a record of DBS checks undertaken and copies of the completed check will be stored electronically in the relevant staff, board or volunteer file.

3.5 ESCV complies with the requirements of company law, and records are maintained and retained in accordance with the retention summary below.



- 3.6 Insurance policies and employer's liability insurance certificates and records relating to the ownership or leasehold of premises are securely stored and retained in line with the retention summary below.
- 3.7 Confidential hard copy records that are waiting to be destroyed should be stored securely in a secure disposal bin located in the ESCV office, which are then regularly shredded or disposed of using a reputable company.
- 3.8 Any organisational assets (electronic devices or storage media) should be appropriately cleared of personal information in advance of or at the point of disposal (by a reputable company), and an appropriate record of disposal obtained and retained.
- 3.9 Any personal assets (electronic devices or storage media) used to access organisational systems should be appropriately cleared of all personal information and records in advance of a role with ESCV coming to an end.

#### 4 Monitoring and review

- 4.1 The Board of East Sussex Community Voice has the ultimate responsibility for implementing and reviewing this policy. The Board will scrutinise our work on data protection and record retention to ensure that we meet our legal, ethical and operational commitments.
- 4.2 The East Sussex Community Voice Chief Executive holds the day-to-day responsibility for ensuring that this policy is implemented.
- 4.3 All staff, board members, volunteers or commissioned providers that deal with personal data are responsible for processing this data in full compliance with the relevant East Sussex Community Voice CIC policies and procedures.
- 4.4 This policy will be reviewed and updated on a two-year rolling basis by the East Sussex Community Voice Board.
- 4.5 All records relevant to administering this policy and procedure will be maintained for a period of 5 years, unless there are exceptional circumstances, and these will be authorised by the Chief Executive.
- 4.6 This policy may be revised sooner if there is a change in working premises, conditions or laws directly affecting data protection, record retention or any other aspect embedded in the document.


#### 5 Approval and Adoption

<b>Author</b>	Simon Kiley, Head of Evidence & Insight
<b>Sponsor</b>	Veronica Kirwan, Chief Executive
<b>Date of approval and adoption</b>	27 <sup>th</sup> March 2024



Date of next scheduled review	March 2026
-------------------------------	------------

**Signature of East Sussex Community Voice CIC Board Chair**

Name	Keith Stevens
Signature	
Date	22nd March 2024



## Retention Schedule for East Sussex Community Voice CIC

### Retention of records in East Sussex Community Voice CIC.

**Employment:** Staff, board and volunteer records should be retained for six years after the end of employment but need only to contain sufficient information to provide a reference (e.g. training and disciplinary records).

Copies of any reference should be retained for six years after the reference request.

Director's files should be kept for six years.

### Employment (Staff, Board, Volunteers and contractors)

Application form and selection material (unsuccessful candidates) (Staff/Board/Volunteers)	One year after interview date
Application form and selection material (Staff/Board/Volunteers)	Duration of employment/participation
References given/information to enable a reference to be provided (Staff)	Six years from the end of employment
References received (Staff/Board/Volunteers)	Duration of employment/paticipation
Annual appraisal, supervision and assessment records	Six years from the end of employment
Sickness and maternity records (Staff)	Six years from the end of employment
Annual leave records (Staff)	Six years from the end of employment
Unpaid leave/special leave records (Staff)	Six years from the end of employment
Records relating to an injury or accident at work (Staff)	12 years
Disciplinary records (Staff)	Six years after employment has ended
Statutory maternity pay records, calculations and certificates (Staff)	Three years after the end of the tax year in which the maternity period ends
Redundancy details, calculation of payments and refunds (Staff)	Seven years from the date of redundancy



**Photo/Media consent forms  
(Staff/Board/Volunteers)**

Six years from the end of  
employment/participation

Note: if an allegation has been made about the member of staff, volunteer or trustee, the staff record should be retained until they reach the normal retirement age or for ten years, if that is longer. E.g. around Safeguarding.

**Public experience, e.g. observations, interviews, enter and view notes, surveys, research/engagement project data.**

**Comments recorded on internal  
databases and project records**

Five years from date of entry

**Any paper-based comments recorded on  
ESCV systems (SmartSurvey/Feedback  
Centre).**

One year from date of entry  
(This is in case there is a query regarding  
an entry on ESCV systems)

**Comments and or other evidence that  
have not been recorded on the ESCV  
systems.**

Five years from date of entry

**Signed consent forms**

Five years from date of collection

**Contact details**

**Mailing lists  
(MailChimp - HWES newsletter sign-up)**

Retain until unsubscribed, request for  
deletion, notified of change or cleaned  
due to non-receipt of emails/responses.

**Outlook contacts (Day-to-day contacts)**

Retain until we receive a request to  
delete or are notified of a change of  
contact details.

**Emails**

Seven years from date of receipt

**DBS checks**

Record disclosure reference number and date of the check (via scan of form stored in the individuals personnel folder) and return to the staff member, board member or volunteer.



## Safeguarding concern recording forms

All safeguarding concern forms and related information should be kept for ten years.

If the record relates to children and young people, it must be kept until they are 21 years old before destruction.

## Financial records

Income tax and National Insurance returns, income tax records and correspondence with HMRC	Six years (public-funded companies)
Payroll records (also overtime, bonuses, expenses)	Not less than six years after the end of the financial year to which they relate
Pension contribution records	Seven years
Pension Scheme Investment Policies	12 years from any benefit payable under the policy

## Corporate

Employers liability certificate	40 years
Insurance policies	Permanently
Certificate of incorporation	Permanently
Minutes of Board of Directors	Permanently
Memorandum of Association	Original to be kept permanently
Articles of association	Original to be kept permanently
Variations to the governing documents	Variations to be kept permanently
Statutory registers	Permanently
Rental or hire purchase agreements	Six years after expiry

## Others



<b>Deeds of title</b>	Permanently
<b>Leases</b>	12 years after the lease has expired
<b>Accident Books</b>	Three years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21).
<b>Health and Safety policy documents</b>	Retain until superseded
<b>Assessment of Risks under Health and Safety Legislation</b>	Retain until superseded



## Appendix 1 - Terms and Definitions

**General Data Protection Regulation (GDPR):** The [Data Protection Act 2018](#) controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).

**Data Controller:** the entity that determines the purposes, conditions and means of the processing of personal data

**Data Processor:** the entity that processes data on behalf of the Data Controller

**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 United Kingdom

**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.