

East Sussex Community Voice

Confidentiality Policy

Policy Schedule

Version	Date of next review by ESCV Board	Date of adoption by ESCV Board
1	n/a	August 2025
2	August 2027	
3		
4		
5		

1. Introduction

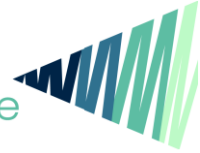
- 1.1 Whilst working at East Sussex Community Voice staff members may have access to, or be entrusted with, confidential information about the organisation, its staff, board members, volunteers or partner organisations as well as information about members of the public who access our services.
- 1.2 We recognise that access to confidential information may vary based on individual's roles. Our confidentiality policy sets out guidance and the procedures that should be followed in relation to confidential information.
- 1.3 The policy applies to all staff, board members, volunteers, sub-contractors and partner organisations.
- 1.4 Related ESCV policies to be read in line with our confidentiality policy can be found at the end of this document.

2 What is confidential information?

- 2.1 Confidential information is defined as any information that could be regarded as 'private'. It is information about an individual, group of people or organisation and is not meant for public or general knowledge.

It may also be any information that is commercially sensitive, such as organisational finances, client details, contract values etc.

- 2.2 The following provide a non-exhaustive list of examples of information that may be 'confidential':

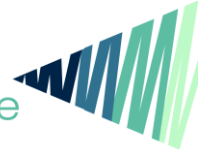


- ESCV employee, board member or volunteer home addresses, contact details or information kept in their personnel files or Bright HR account.
- Information provided by the Disclosure and Barring service (DBS).
- Individual participant or user's names, home addresses, telephone numbers and e-mail addresses.
- Any personal information concerning an individual participant or user's circumstances that are disclosed to a member of staff during their work.
- Sensitive information concerning the operation or funding of statutory or voluntary organisations disclosed to ESCV staff during their work.
- Financial information (such as funding proposals, contracts with suppliers, correspondence and negotiations with funders) other than that which is required to be published in ESCV's audited accounts and/or annual report or required by funders for monitoring purposes.
- Opinions expressed in debate, and not formally recorded (e.g. in agreed minutes), by staff, board members or volunteers of ESCV.

3 Procedures for dealing with confidential information

3.1 Overarching principles of confidentiality

- Confidential information will not be sought from a member of the public unless expressly in the interests of that person e.g. to help in signposting appropriately or enable better service delivery.
- No personal information about staff, volunteers or members of the public will be given to any third party including a member of their family, without consent.
- In no circumstances will details of a member of the public client be discussed with anyone outside of the organisation, or in a public area in such a manner that it is possible to identify that person.
- Staff, board members and volunteers should take due care and attention when speaking to members of the public and using the telephone. No member of the public should be able to hear a conversation or personal details of another service user.
- Where confidential information needs to be shared internally (to



deliver a service or fulfil a business function), GDPR principles and best practice will be followed.

- ESCV board members, volunteers and staff may attend meetings where confidential information is discussed. Anyone working for or representing ESCV, whether in a paid or unpaid capacity, will respect the bounds of confidentiality of that meeting, whether this be regarding individuals, commissioning or services.

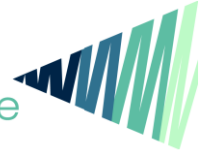
3.2 Individual Users (ESCV service users, participants, and representatives):

- All information concerning individuals should be stored in such a way as to comply with contemporary data protection regulations and ESCV policies (including Data in Transit; Data Protection; Statement on the Secure Storage of Data).
- Information concerning individuals should not normally be removed from ESCV's offices. It may be necessary at times for an employee/volunteer involved in outreach work and home working to take records home temporarily if they are unable to return to the office.
- All information removed from the office must be kept safe and secure (including during transportation) until returned to the ESCV office or securely disposed of.
- Information concerning individuals should not be left unsecured, open to view or unattended on desks or in the photocopier.

3.3 Staff

- All personnel information should be stored on the ESCV SharePoint system in individual staff folders with restricted permission levels or on Bright HR. No hard copy records should be retained or stored in the ESCV office or elsewhere.
- Access to personnel files should be limited to those with a legitimate business need to access such information, including the relevant staff member, their line manager, the Senior Leadership Team and the Business Support Officer.
- Disposal of personnel files or staff information should adhere to the timescales outlined in the ESCV Record Keeping and Retention Policy.

3.4 Financial



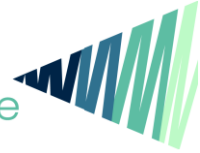
- The organisation's auditor or his/her authorised representative will have access to all the organisation's financial records in line with financial regulations.
- No financial information of a confidential nature shall be removed from ESCV offices or systems without the permission of the Chief Executive, Chair of the Board, or Lead Board member for Finance.
- Contracts, salary and pension information, bank statements, expenses and other confidential or commercially sensitive information must be securely stored at all times.

4 Additional procedures

- 4.1 Staff working at home or away from the ESCV office must ensure the safe keeping of all confidential documents or information following the procedures outlined above. This includes documents stored on laptops, phones, memory devices and items stored on cloud-based services such as SharePoint and OneDrive.
- 4.2 Before the end of an employee's term of employment, all documents or information in the employee's possession belonging to the organisation, including documentation made during employment, should be returned to their line manager.
- 4.3 Before leaving ESCV, all board members and volunteers should return all documents or information in their possession belonging to the organisation to the Engagement Manager (Volunteering) or Business Support Officer.
- 4.4 Staff should seek guidance from the Chief Executive or line manager if they unclear which documents or information should be treated as 'confidential'.
- 4.5 It is the responsibility of all employees to ensure that where personal information needs to be shared outside ESCV on behalf of service users that appropriate consent is obtained from those concerned and is recorded before any information is relayed.

5 Limits to confidentiality

- 5.1 East Sussex Community Voice recognises occasions arise where employees/board members/volunteers may feel they need to breach confidentiality. Any breach of confidentiality may damage the reputation of the organisation and must be treated very seriously. If confidentiality is breached without recourse to the following procedure, disciplinary action may be taken.



- 5.2 If you tell us something which leads us to believe you or someone else may be at risk of serious harm or abuse, or assisting a serious criminal offence, ESCV reserves the right to break confidentiality should this be deemed necessary.

These circumstances may include:

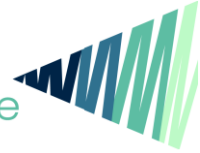
- If a member of staff, board member or volunteer believes that a member of the public could cause danger to themselves or to others
- If a member of staff, board member or volunteer suspects abuse or has knowledge of abuse
- If the member of the public gives information which indicates that a crime has been committed
- If disclosure is required by law, for example, by the police
- If a person is felt to lack the mental capacity to make a decision. In such cases staff or volunteers will discuss with a manager and they will only act in the person's best interest
- If the caller gives information which indicates a possible terrorist threat

- 5.3 On occasions where an ESCV employee, board member or volunteer feels confidentiality should be breached, the following steps must be taken:

- The individual should raise the matter immediately with their line manager, or if they are unavailable, the Chief Executive or Chair of the Board.
- The individual must discuss the issues involved and explain why they feel confidentiality should be breached and what would be achieved. The line manager/Chief Executive/Board Chair should make a written record of this discussion.
- The line manager should discuss with the individual what options are available.

- 5.4 The line manager (or alternate - see above) is responsible for deciding whether confidentiality should be breached, and if they make this decision, they should take the following steps:

- The line manager should contact the Chief Executive/Board Chair and brief them on the full facts of the case.
- If the Chief Executive/Board Chair agrees to breaching confidentiality, a full written report on the case should be made. The line manager is responsible for ensuring all necessary actions take place.



- If the CEO/Board Chair does not agree to breach confidentiality, then this is the final decision.

5.5 Unauthorised breaches of ESCV's confidentiality procedures will be dealt with under the Disciplinary Procedure. Major breaches may constitute gross misconduct. This includes breaches where there is a deliberate intention to cause harm or major inconvenience to the organisation, a member of staff, or an individual of the organisation.

5.6 Gross negligence may apply where the harm that may occur is not foreseen due to a failure to follow the procedure set out in this policy.

6 Access to personal information

6.1 All members of the public, staff, board members and volunteers have the right to request access to all information stored about them, under powers enshrined in the Data Protection Act, and have a right to see a copy of this confidentiality policy on request.

7 Monitoring and review

7.1 The Board of East Sussex Community Voice has the ultimate responsibility for implementing and reviewing this policy. The Board will scrutinise our work on disclosure to ensure that we meet our legal, ethical and operational commitments.

7.2 The East Sussex Community Voice Chief Executive holds the day-to-day responsibility for ensuring that this policy is implemented.

7.3 This policy will be reviewed and updated on a two-year rolling basis by the East Sussex Community Voice Board.

7.4 This policy may be revised sooner if there is a change in working premises, conditions or laws directly affecting disclosure or any other aspect embedded in the document.

8 Related Policies

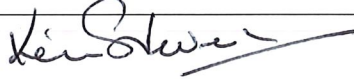
- 8.1 The following policies and procedures that are related to this policy include:
- Data in Transit
 - Data Protection
 - Record Keeping and Retention Policy
 - Statement on the Secure Storage of Data



8.2 Approval and Adoption

Author/Reviewer	SIMON KILEY
Sponsor	ALEX HAWKINS
Date of approval and adoption	AUGUST 2025
Date of next scheduled review	AUGUST 2027

Signature of East Sussex Community Voice CIC Board Chair

Name	KEITH STEVENS
Signature	
Date	21/08/25