East Sussex Community Voice

Data in Transit Policy

Policy Schedule

Version	Date of next review by ESCV Board	Date of adoption by ESCV Board
1	n/a	28th September 2020
2	28th September 2022	March 2024
3	May 2026	28th May 2026
4	May 2028	
5		

1 Introduction

1.1 This policy seeks to minimise the unauthorised disclosure of information by setting out clear standards of practice for East Sussex Community Voice (ESCV) in using, receiving or sending sensitive or confidential data.

1.2 The potential impacts of a loss or disclosure of sensitive or confidential data may be determined by the degree of sensitivity of the data and the quantity involved. However, a single record can have a potentially massive impact on an individual or the organisation if accidentally lost or disclosed to others.

1.3 Our duty to protect the information of individuals and the organisation arises from legislation relating to information security, including:

- General Data Protection Regulation [GDPR]
- Data Protection Act 2018
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Human Rights Act 2000

1.4 This policy covers all circumstances where sensitive or confidential data are taken outside of their normally secure location. This includes data in all formats – non-electronic (paper) and electronic (e.g. on PCs, tablets, laptops and removable storage media – e.g. USB memory sticks, phones etc.).

1.5 It applies to all our employees, board members, volunteers, contractors, and partners who access our network, computers, mobile devices, platforms and other IT equipment. Hereafter, all parties will be referred to as 'employees' in this policy.

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

1.6 All employees should be aware of their responsibilities under this policy and of the measures set out below to comply with it.

2 Definitions

2.1 What is sensitive and confidential data?

The following list is not exhaustive and contains examples of sensitive and confidential data:

- Any data marked Confidential/Official/Sensitive/Protected/Restricted (see Appendix 1 Glossary)
- Any data covered by the Data Protection Act - i.e. all data that relates to a living individual.
- Any data classified as 'Commercial in Confidence' - e.g. data that relates to commercial proposals or current negotiations.
- Any data relating to security information, investigations and proceedings, information provided in confidence etc.

An easy sense-check on whether data is sensitive or confidential is to ask:

- Is the data covered by the Data Protection Act 2018?
- Could release of the information cause problems or damage to individuals, the public, ESCV, or, a partner organisation? This could be personal, financial, reputation or legal damage.
- Could release prejudice the outcome of negotiations or investigations?

A list of further definitions is included at the end of this document to explain some of the terms used. See Appendix 1.

If in doubt, ask the Chief Executive or Data Protection Lead and err on the side of caution, treating information as sensitive and confidential until you can confirm otherwise.

2.2 What are 'normally secure locations'?

These may include:

- A secure network/storage facility with:
    - Access controls such as individual login accounts or two-factor authentication
    - Backup and recovery facilities
    - No public access
    - Anti-virus and firewall protection

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

Examples are: The ESCV SharePoint network

- Secure buildings or parts of buildings with:
    - Physical access controls - swipe cards, keys etc.
    - No public access
    - Lockable storage facilities
    - Other protection systems e.g.: alarms, CCTV, time locks etc.

Examples are: The ESCV Office (excluding public access areas)

3 Access and authorisation

3.1 No employee shall be given access to ESCV ICT hardware, software and systems who has not previously been authorised to do so by the Chief Executive or a senior manager.

3.2 All account information and hardware resources allocated to employees will be recorded in appropriate organisational asset logs.

3.3 No employee shall be given access to personal or sensitive information who has not previously been authorised to do so by the Chief Executive or a senior manager. The data protection lead will be consulted before any sharing occurs.

4 Responsibilities

4.1 ESCV maintains appropriate security and privacy of data and will ensure that appropriate tools, training and guidance are available to employees, including:

- A secure network for storing and using electronic data
- Secure work locations for storing, using and disposing of hard-copy data
- Advice and support over the use of personal data

4.2 Employees will act in accordance with the following standards and guidance to ensure security and privacy of sensitive and confidential data outside of its normally secure location.

4.3 Organisations that use our data to help us deliver a service/project may have to confirm they comply with these or equivalent standards.

5 Disciplinary and other sanctions

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

5.1 ESCV considers this policy and the protection of personal and organisational data to be extremely important. Where ESCV employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably.

5.2 If employees are found to be in breach of the policy and its guidance, they may be subject to disciplinary procedures.

6 Volunteers

6.1 As specified in 1.5, this policy applies to any volunteers undertaking activities on behalf of ESCV, its programmes, or projects.

6.2 All volunteers undertaking activities requiring access to personal or sensitive information will receive appropriate data protection training or guidance before commencing any activity.

6.3 Staff will only share with volunteers the minimum personal or sensitive information required to complete the task.

6.4 Sharing of personal or sensitive information from staff to volunteers, and volunteers to staff, will be undertaken through secure means e.g. encrypted emails, password protected files, recorded post etc.

6.5 When undertaking activities that require access to personal or sensitive information, volunteers must:

- only used it for the specific purposes of the activities being undertaken
- store personal or sensitive information securely and not allow unauthorised access to either paper or hard copies
- not copy or duplicate any personal or sensitive information shared with them
- ensure all copies of personal or sensitive information are returned to staff or securely deleted/disposed of, when an activity is completed, or their role ends. This includes from personal computers and mobile phones.

6.6 Volunteers should contact the Volunteer Manager or Chief Executive as soon as possible if:

- they receive a query/complaint in relation to the handling of someone's personal information (including Subject Access Requests or Freedom of Information requests)

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

- any data breaches (losses or accidental sharing) or near misses involving personal and sensitive data occur, this applies equally to both paper and electronic copies

7 'Common Sense' Precautions

7.1 There are some 'common sense' precautions that may be taken before sending or receiving sensitive or confidential data, including:

- Checking you are not sending/receiving more detail than is necessary i.e. will the information still meet the need if you remove the sensitive material or aggregate the data? (GDPR Principle: Data Minimisation).
- Checking the data you are sending/receiving is correct and appropriate (GDPR Principle: Data Accuracy)
- Checking you are sending the data to the correct person/address.
- Checking how you intend to keep it secure (GDPR Principle: Integrity and confidentiality).

7.2 It is the sender's responsibility to ensure the method used to transfer data and the degree of security is appropriate to the sensitivity, quantity and potential impact of loss of the data being handled.

8 Organisational email

8.1 Emailing information between internal ESCV mailboxes is secure. However, following best practice, you should always link or reference information rather than attaching a copy where possible.

8.2 If you are sending sensitive or confidential data by email to an external address (other than a secure address) you must:

- Send them as an encrypted email using an appropriate encryption solution.
- Make sure the recipient is correct, known and trustworthy before sending.

9 Web Interface

9.1 If you are transferring sensitive or confidential data through a web portal you must:

- Ensure there is robust access control in place (i.e. unique username/password)
- Ensure only the people who need the data can see them
- Ensure data is encrypted (https connection or equivalent)

10 Mobile Storage Devices

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

10.1 If you are taking data with you on a mobile storage device, such as a tablet PC, laptop, digital camera, smart phone or a USB memory stick you must:

- Make sure there is no other more secure option available to you
- Only use an ESCV approved device i.e. provided by the organisation
- Take only as much as necessary, for as long as necessary and transfer them back to their normally secure location as soon as possible
- Keep the decryption PIN, password or token securely and separately from the device/data
- Do not take equipment outside of the UK without approval from the ESCV Chief Executive

10.2 **Take all reasonable precautions to keep the device and data safe and secure e.g.:**

- Keep it with you whenever possible; lock it away securely when you are not able
- Never leave it in plain sight in public places
- Never let others use your access or device
- Delete the data from the device as soon as possible
- Report loss/theft immediately

11 Post

11.1 The postal service is considered reasonably secure for small amounts or low impact data (i.e. records pertaining to an individual, but NOT including very sensitive personal data).

As a minimum, precautions you must take to prevent loss include:

- Make sure the recipient and destination address is correct, accurate and up-to-date
- Clearly mark the envelope/parcel with a return address in case of incorrect delivery
- Do not send the only copy of the data if it is practical to make and retain a duplicate. *You must assess the impact of loss of the original and make a copy if that impact is unacceptable*
- If you use a courier they must be a known and trusted company or supplier
- Consider using recorded/registered post when sending sensitive information
- Make sure it is traceable (i.e. confirmation of receipt)
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

12 Use of personal IT

12.1 If you are working at home, on your own equipment or using a personal online service you must:

- Use a device that has up to date internet security protection in place
- Not transfer sensitive or confidential data to your home PC, laptop or personal online service (e.g. Gmail account, Dropbox etc.)
- Only have as much sensitive or confidential information open as necessary and only for as long as necessary - **do not** save the data on your device
- Always save the data back to their normally secure location when you have finished
- You must not leave the device unattended for any period of time such that others can access any sensitive data; always lock the device or log out when you are not using it
- Not connect your device to an insecure or unknown network when accessing sensitive or confidential information.

13 Physical (Paper) records

13.1 If you are taking sensitive or confidential information with you in non-electronic (paper) format you must:

- Make sure there is no other option available to you
- Never take the only copy with you if it is practical to make and retain a duplicate. You must assess the impact of loss of the original and make a copy if that impact is unacceptable (where copies are made, ensure these are securely destroyed as soon as possible following their use).
- Take only as much as necessary and only for as long as necessary
- Transfer it back to its normally secure location as soon as reasonably possible

13.2 Take all reasonable precautions to keep the records safe and secure e.g.:

- Keep them with you whenever possible; lock them away securely when you are not able
- Use a suitable container that prevents accidental loss and/or viewing by others
- Never leave them in plain sight in public places
- Report loss/theft immediately

14 Prohibited data handling activities

14.1 There are some data handling activities which are prohibited for employees:

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

- Never share your network password with anyone and use a different password when encrypting/protecting files.
- Sending sensitive or confidential information in unencrypted electronic form without taking appropriate precautions as set out in this policy and guidance.
- Storing sensitive or confidential data on any personal or non-organisational equipment or in unencrypted/unprotected form.
- Sending sensitive or confidential information as unsecured physical records.
- Working on sensitive or confidential data on a public device (for example, in a library or cafe).
- Working on sensitive or confidential data on a device with an unencrypted wireless (WiFi) connection, i.e. ensure your home wireless network has encryption and use it.
- Leaving sensitive or confidential physical records in plain view of others (i.e. unattended in your office, on the back seat of your car, in a public place, on your kitchen table or even with you, but where they can be overlooked by others).
- Leaving any device holding sensitive or confidential information unattended in a non-secure environment.
- Leaving any device holding sensitive or confidential information in a vehicle overnight

15 Reporting data loss

15.1 Staff should report any loss (or 'near miss') of sensitive and/or confidential data to the Chief Executive/Deputy Chief Executive and Data Protection Lead as soon as possible and complete a data breach incident report form.

See the ESCV Data Breach Procedure for more information and details of the reporting process.

16 Other Relevant Policies and Guidance

16.1 This policy should be read and acted upon in conjunction with the ESCV:

- Data Protection and Information Security Policy
- Privacy Policy
- Record Keeping and Retention Policy

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

17 Compliance, monitoring and review

17.1 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 to ensure that we meet our legal, ethical and operational commitments.

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

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

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

18 Approval and Adoption

Author/Reviewer	Simon Kiley, Deputy Chief Executive
Sponsor	Veronica Kirwan, Chief Executive
Date of approval and adoption	21st May 2026
Date of next scheduled review	May 2028

Signature of East Sussex Community Voice CIC Board Chair

Name	**Vanessa Taylor**
Signature	
Date	**22.06.26**

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk

Appendix 1 – Glossary

Personal Data
Personal data is anything that relates to a living individual in which the individual can be identified directly from the information from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Special Category Personal Data
Defined as being any personal data relating to racial or ethnic origin, political opinions, religious or similar beliefs, membership of a trade union, physical or mental health or condition, sexual life, the commission or alleged commission of any offence, any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

East Sussex Community Voice, Unit 31, The Old Printworks, 1 Commercial Rd, Eastbourne BN21 3XQ
Registered Company No: 08270069
email: info@escv.org.uk