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	
3		
4		
5		

Key points:

- All employees, board members, volunteers and contracted parties are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data is protected.
- All sensitive and confidential electronic data being taken outside of its normally secure location must be appropriate protected or encrypted.
- Data loss must be reported immediately to the Director and Data Protection Officer.
- Disciplinary action could be taken where employees do not follow the guidance set out in this Policy.

1. Introduction

1.1 Sensitive and confidential data must be treated with appropriate security by all who handle them. 'Appropriate' is not defined in terms of hard and fast rules, but is meant to be a degree of precaution and security proportionate to the potential impact of accidental disclosure. It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore staff handling sensitive and confidential data MUST assume personal responsibility and make considered judgements in terms of how they handle data and if in any doubt, seek support from the Data Protection Officer.

1.2 Overall impact is determined by the degree of sensitivity of the data and the quantity involved, but it is important to remember that a single record about an individual can have a potentially massive impact on that individual if accidentally disclosed to others.

1.3 Consider: If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone - what would

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

you do to protect it?

2. Purpose

2.1 This document is intended to prevent unauthorised disclosure of information by setting out clear standards of practice to maintain good security when using, taking or sending sensitive or confidential data outside of their normally secure location.

2.2 The need for this is driven by our duty to protect the information of individuals and the organisation. This duty arises from legislation relating to information security, the most notable of which is as follows;

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

2.3 A list of definitions is included at the end of this policy document to explain some of the terms used.

3. Other Relevant Policies and Guidance

3.1 This policy does not stand alone, but should be read and acted upon in conjunction with the organisations:

- Data Protection [and Information Security] Policy
- Acceptable Use Agreements
- Code of Conduct
- Others as necessary

4. Scope and who the policy applies to

4.1 The scope 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.).

4.2 Whilst the Policy refers to employees, board members and volunteers, it also applies to temporary staff, secondees, work experience candidates, and all staff of service delivery partners and other agencies that process our data.

5. Responsibilities

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

5.1 The organisation maintains appropriate security and privacy of data that it uses to perform its functions and it will ensure that appropriate tools, training and guidance are available to staff and members i.e.:

- Secure network for storing and using electronic data
- Secure work locations for storing and using hard-copy data
- Encryption tools for transmission of data outside secure locations

5.2 Staff, board members and volunteers will act in accordance with the following standards and guidance to ensure security and privacy of sensitive and confidential data outside of their normally secure location.

5.3 Organisations that use our data to help us deliver a service will have to confirm they comply with these or equivalent standards.

6. Disciplinary and other sanctions

6.1 The organisation considers this policy and the protection of personal data to be extremely important.

6.2 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.

6.3 However, if ESCV employees are found to be in breach of the policy and its guidance then they may be subject to disciplinary procedures up to and including dismissal.

7. 'Common Sense' Precautions

7.1 There are some 'common sense' precautions that may be taken before sending or taking sensitive or confidential data outside of their normally secure location, these are:

- Check that you are not sending/taking 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)
- Check that the data you are sending/taking are correct and appropriate. (GDPR Principle: Data Accuracy)
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure. (GDPR Principle: Integrity and confidentiality)

7.2 It is your responsibility to ensure that the method used to transfer data and the degree of security is appropriate to the sensitivity, quantity and

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

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

9. Web Interface

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

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

10. Mobile Storage Devices

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 that 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 Director

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 can't
- 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

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

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).

Please refer to any specific organisational guidance on use of the postal service. As a minimum, there are precautions that you must take to prevent loss:

- Make sure that 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 known and trusted
- 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

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

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

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

- Make sure that 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 can't
- 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. Fax

14.1 Sending sensitive or confidential information by fax is a last resort and should only be used if the need is urgent and there is no alternative available and you must:

- Use a Fax to E-Mail solution where available
- Make sure the receiving fax machine is in a secure environment
- Make sure the recipient is there to receive it at the time of arrival and that they are known and trusted
- Make sure it is traceable (e.g. confirmation of receipt)

15. You must not!

15.1 There are some data handling activities which are prohibited:

- Never share your network password with anyone and use a different password when encrypting 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 form.

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

- 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

16. Reporting data loss

16.1 Staff should report a loss of sensitive and/or confidential data to the Director as soon as possible and complete a data breach incident report form. See the Data Breach Procedure for more information and details of the reporting process.

17. Definitions

17.1 Sensitive and confidential data

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

- Any data that is marked Official Sensitive/Protect/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, the organisation, or, a partner organisation? This could be personal, financial, reputation or legal damage.

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk

- Could release prejudice the outcome of negotiations or investigations?

If in doubt ask the Director or Data Protection Officer and err on the side of caution - treat them as sensitive and confidential - do not assume that they are not.

17.2 Normally Secure Location

For the purposes of this policy standard 'normally secure location' is defined as:

- A secure network/storage facility with:
- Access controls such as individual login accounts
- Backup and recovery facilities
- No public access
- Anti-virus and firewall protection
- Examples are:
  - The ESCV network
  - ESCV administrative networks
- 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:
    - Administrative areas (excluding public access areas)

18. Last Word – Remember:

18.1 If you were working on very sensitive and private information about yourself, carrying it with you or sending it to someone what would you do to protect it?

East Sussex Community Voice, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
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, Barbican Suite, Greencoat House, 32 St Leonards Road, Eastbourne, East Sussex, BN21 3UT
Registered Company No: 08270069
email: info@escv.org.uk