eastsussex.gov.uk

East Sussex
County Council

Data in Transit Policy
June 2019
Version 4.0

Data in Transit Policy

Summary

This policy describes clear standards of practice to maintain good security when using, taking or sending sensitive or confidential council data outside of their normally secure location

Contents

Document Owner/Contact: East Sussex County Council Information Governance Lead.
Date Created: September 2012.
Date last reviewed: June 2019.
Version: 4.0.
Next Review Due: March 2020.
Target Audience: All ESCC network users.
Document Approved By: Senior Information Risk Owner.
Approval date: 19 March 2018.

This document forms part of a suite of Information Management Policy and Guidance.

Data in Transit Policy

Key points:

• All Council employees and elected Members are personally responsible for taking reasonable and appropriate precautions to ensure that all sensitive and confidential data, including personal data, is protected.
• All sensitive and confidential electronic data being taken outside of its normally secure location must be encrypted.
• Data loss must be reported immediately to your line manager.
• Disciplinary action will be taken where Council 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 whilst delivering their service and if in any doubt seek support from their line manager or Information Governance Officer.

1.2 Overall impact is determined by the degree of sensitivity of the data and the quantity of data involved, but we must 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 you do to protect it?

2. Purpose

2.1 This document is intended to prevent unauthorised disclosure of information by laying down 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 personal data of individuals handled by East Sussex County Council. This duty arises from legislation relating to information security, the most notable of which is as follows;

- Data Protection Act 2018
- General Data Protection Regulation
- 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 Council's:

- Data in Transit Guidance
- Data Protection Guidance - Guidance for Employees
- E-Mail Use Policy
- Information Security Policy
- Using Technology to work remotely

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).

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

5. Responsibilities

5.1 ESCC 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 ESCC staff and elected members 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 Service delivery partners and other agencies that use our data for our service delivery will have to confirm they comply with these or equivalent standards.

5.4 Where information sharing protocols and agreements are already in place for your service area you must act in accordance with the security standards specified in such agreements where they exceed those of this policy. In all other respects you must work to the standards set out in this policy.

6. Disciplinary and other sanctions

6.1 The Council considers this policy to be extremely important.

6.2 Where Council 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 Council 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 you can take 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?
- Check that the data you are sending/taking are correct and appropriate.
- Check that you are sending the data to the correct person/address.
- Check how you intend to keep it secure.
- Do not send or forward emails containing sensitive or personally identifiable information to your personal email account

8. Approved secure transfer mechanisms

The following data transfer methods are ranked in order of security and it is your responsibility to ensure that you use a method and degree of security appropriate to the sensitivity, quantity and potential impact of loss of the data being handled.

- ESCC Secure Email
- AVCO Any Comms (software that allows secure transfer of documents to schools)
- NHS Mail
- Secure FTP
- Royal Mail Recorded Delivery

(This list is not exhaustive and other secure mechanisms will be added, if in doubt ask your manager or the Information Security Team).

9. ESCC email

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

9.2 If you are sending sensitive or confidential data by email to an external address, other than to Police, NHS, DWP, CAFCAS and Youth Justice Services, (which will automatically be sent encrypted), you must;

- Send them as an encrypted email using the ESCC encryption solution
- Secure Mail – refer to Secure Email guidance on the Intranet.
- Make sure the recipient is correct, known and trustworthy

10. Web Interface

10.1 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 - (includes a padlock in the address bar))
- Ensure you are using ESCC equipment

11. Mobile Storage Devices

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

- Make sure that there is no other more secure option available to you
- Only use an ESCC approved device
- Take only as much data 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 (where applicable)
- Do not take Council equipment outside of the UK without approval from IT&D
- 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

12. Post

12.1 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 departmental/team

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. This is especially important when using the auto-complete function which displays suggested email addresses from emails previously sent.
- 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)
- Where possible inform addressee of time, date and means by which information is being sent
- Physical records must be sent in a suitable container i.e. robust and secure enough to prevent accidental loss and/or tampering

13. Use of personal IT

13.1 Use of personal IT **should only be used in exceptional circumstances. ESCC equipment should *always* be used when processing personal data.**

If, in exceptional circumstances, it is necessary to use your own equipment or use a personal online service you must:

- Use a device that has up to date internet security protection in place
- Use initials instead of any personal data if required
- 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; always lock the device or log out when you are not using it
- Not connect your device to an insecure or unknown network

14. Physical (Paper) records

14.1 If you are taking sensitive or confidential information (including any personal 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
- 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

15. Fax

15.1 Sending personal 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:

- Never send highly sensitive information by fax
- Use the ESCC Fax to E-Mail solution where available
- Send a test fax to ensure the number is correct where possible
- 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). A log must be kept of all confidential faxes sent and received giving details of sender and recipient, date and time of fax and a copy of the machine's log confirming status of the transmission.

16. You must not!

16.1 There are some data handling activities which are prohibited:

- Never share your network password with anyone and always 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.
- Sending or forwarding sensitive or confidential information (including personally identifiable information) to personal email addresses
- Storing sensitive or confidential data on any personal or non-ESCC equipment or in unencrypted 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 an ESCC device with an unencrypted wireless (WiFi) connection without using VPN and ensuring the wireless network has encryption.
- 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 or paperwork holding sensitive or confidential information in a vehicle overnight

17. Reporting data loss

17.1 Staff should report a loss of sensitive and/or confidential data to their line manager and complete an information security incident form, available on the intranet. See the Information Security Incident Policy and Procedure for more information and details of the reporting process

18. Definitions

18.1 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/General Data Protection Regulation (GDPR) - 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 held on 'pink papers' - i.e. cabinet papers containing organisationally or publicly sensitive information.
- 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:

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

If in doubt, ask your manager and err on the side of caution - treat them as sensitive and confidential - do not assume that they are not.

18.2 Normally Secure Location

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

a) 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 ESCC corporate network

b) 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:

- ESCC County Hall (excluding public access areas)
- St Mary's House (excluding public access areas)

19. Last Word – Remember:

19.1 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?

20. Related Policies and Guidance

- Data Protection and Information Security Policy
- Data in Transit Guidance
- E-mail Use Policy
- Using Technology to Work Remotely
- Sending secure e-mail (intranet content)

Appendix 1 – Glossary

Personal Data
Personal data is information relating to living individuals who:

- can be identified or who are identifiable directly from data/information; or
- who can be indirectly identified from that information in combination with other information.

Protective Marking
Terms used to identify the confidentiality/sensitivity of information. Previous classification has used the terms: Restrict, Protect, Unclassified. Current Government Security Classification terms applicable to ESCC: Official- Sensitive Personal, Official – Sensitive Commercial, Official – Disclosable

Sensitive Personal Data (Special Category Data)
Defined under Data Protection Legislation as any data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of uniquely identifying a natural person), data concerning health, data concerning a person's sex life or sexual orientation or data concerning criminal conviction and offences. These are considered to be more sensitive and you may only be processed in more limited circumstances.