



Roselands & Stafford
Federation

Draft Data in Transit Policy

About this document:

<p>Enquiries: Information Governance Team</p> <p>Author: Information Governance Team</p> <p>Telephone: 01273 337610</p> <p>Email: schoolsDPO@eastsussex.gov.uk</p>	<p>Version number: 1</p> <p>Related information</p> <p>School Privacy Notices Data Protection Policy Freedom of Information Policy Records Management Policy</p>
---	--

Document summary

According to the Data Protection Act 2018 (*Schedule 1, Part 4, Paragraph 39*), this document must explain both:

- How the processing of special category data complies with the key data protection principles (as outlined in Article 5 of the GDPR)
- Outline how long this data will be kept for, as well as how it will be erased once it reaches the end of the retention period.

Document control:

Ratification			
Signed by	Name	Signature	Date
Headteacher	John Maxwell		
Chair of Governors	Richard Sage		
Distribution			
Shared with			
<ul style="list-style-type: none"> • Staff via school server • Governors via full governing body meeting • Parents via website 			
Revision history			
Version	Revision Date	Revised By	Revision
1.1	17.10.19	John Maxwell	ESCC model policy adapted as required
Date for next review:			

Contents

Key points:	4
1. Introduction	4
2. Purpose	4
3. Other Relevant Policies and Guidance	4
4. Scope and who the policy applies to	5
5. Responsibilities	5
6. Disciplinary and other sanctions	5
7. 'Common Sense' Precautions	5
8. Approved secure transfer mechanisms	6
9. School email	6
10. Web Interface	6
11. Mobile Storage Devices	6
12. Post	7
13. Use of personal IT	7
14. Physical (Paper) records	8
15. Fax	8
16. Prohibited activities	8
17. Reporting data loss	9
18. Definitions	9
19. Key considerations and reflections:	10
Appendix 1 – Glossary	11

Key points:

- All employees and governors 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 encrypted.
- Data loss must be reported immediately to the headteacher
- 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 their DPO.
- 1.2 Overall impact is determined by the degree of sensitivity of the data and the quantity 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 information of individuals and the school. 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 schools:
 - 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).
- 4.2 Whilst the Policy refers to employees and governors, 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 The school 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 School staff and governors 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 school considers this policy to be extremely important.
- 6.2 Where school 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 school 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? (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 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.

8. Approved secure transfer mechanisms

8.1 These are secure transfer mechanisms in use and approved as secure for the purpose. Examples of this are:

- Secure Email
- AVCO AnyComms (software that allows secure transfer of documents)
- School to School (S2S)
- Public Services Network (PSN formally GCSX)
- N3 (The NHS network) including NHS Mail

If in doubt about the security of communication, ask Sarah Oxenbury or the federation's DPO.

9. School email

9.1 Emailing information between internal school 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 a secure address) you must:

- Send them as an encrypted email using the designated encryption solution. This may be Voltage Secure Mail but you should check with your IT technician.
- Make sure the recipient is correct, known and trustworthy

9.3 For emailing sensitive information to government bodies, use a GCSX/PSN service where available (see guidance for more information).

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)

11. Mobile Storage Devices

11.1 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 a school approved device
- 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 school equipment outside of the UK without approval from ICT

11.2 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

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 school 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

13. Use of personal IT

13.1 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.

14. Physical (Paper) records

14.1 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

14.2 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

15. Fax

15.1 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)

16. Prohibited activities

16.1 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-school 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 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

17. Reporting data loss

17.1 Staff should report a loss of sensitive and/or confidential data to the headteacher and complete a data breach incident report form. See the Data Breach 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 - 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:
 - Are the data covered by the Data Protection Act 2018?
 - Could release of the information cause problems or damage to individuals, the public, the school, 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 headteacher 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 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 school network
 - Schools 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:
 - Schools administrative areas (excluding public access areas)

19. Key considerations and reflections:

- 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? Bearing this question in mind will give you a framework for making decisions in line with the principles of this policy.
- 19.2 If in doubt, ask for advice or support – it is better to do this than to make a choice which may have negative repercussions.

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.