Salisbury Plain
Academies

Secure Data Handling Policy

SALISBURY PLAIN ACADEMIES POLICIES

VERSION CONTROL SHEET

POLICY NAME: Secure Data Handling

Policy Prepared by: Jo Wakeham

Document date	**Filename**	**Mtg submitted**	**Summary of changes required**
May 2018	Secure Data Handling	FAME	

Policy Review Date: April 2021

Contents

This policy should be read and understood in conjunction with the following policies and guidance:

- The Data Protection Act 1998
- Child Protection Policy
- Becta: Information Risk Management and Protective Marking
- Record Management Toolkit for Schools (Version 5, February 2016) (Appendix D)
- Information Sharing: Advice for practitioners providing safeguarding services to children, your people, parents and carers (DfE March 2015) (Appendix E)
- Freedom of Information Procedures and Toolkit

1 Principles

1.1 Colleagues within schools have increasing access to a wide range of sensitive information[1]. There are generally two types of sensitive information; personal data concerning the staff and pupils and commercially sensitive financial data. It is important to ensure that both types of information are managed in a secure way at all times.

1.2 The school recognises that by efficiently managing its data and record keeping it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Trust.

1.3 Data and records provide evidence for protecting the legal rights and interests of the school and provide evidence for demonstrating performance and accountability.

1.4 This policy applies to all data and records created, received or maintained by staff of the school in the course of carrying out its functions.

1.5 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created or maintained in hard copy or electronically.

1.6 The school will make parents/carers and staff aware of the data it holds by providing them with a copy of the DfE documents entitled:

- Privacy notice for pupils
- Privacy notice for school workforce

Personal data is the most likely form of sensitive data that a school will hold. Personal data is defined by the Data Protection Act as ***"Data relating to a living individual who can be identified from the data"***. The Act gives 8 principles to bear in mind when dealing with such information. Data must:

[1] The terms, "Information" and "data" are treated as the same for the purposes of this policy.

- be processed fairly and lawfully
- be collected for a specified purpose and not used for anything incompatible with that purpose
- be adequate, relevant and not excessive
- be accurate and up-to-date
- not be kept longer than necessary
- be processed in accordance with the rights of the data subject
- be kept securely
- not be transferred outside the EEA (European Economic Area) unless the country offers adequate protection.

1.7 The Data Protection Act states that some types of personal information demand an even higher level of protection, this includes information relating to:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life (orientation)
- the commission or alleged commission by them of any offence, or any proceedings for such or the sentence of any court in such proceedings.

1.8 The three questions below can be used to quickly assess whether information needs to treated securely, i.e.

1. Would disclosure / loss place anyone at risk?
2. Would disclosure / loss cause embarrassment to an individual or the school?
3. Would disclosure / loss have legal or financial implications?

If the answer to any of the above is "yes" then it will contain personal or commercially sensitive information and needs a level of protection. (A more detailed assessment guide is contained with Appendix A - Help sheet for assessing risk of sharing information).

2 Responsibilities

2.1 The Trust has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The overall responsibility for this policy is **Salisbury Plain Academies Trust.**

2.2 As a processor of personal data, the Trust has a responsibility to register with the 'Information Commissioner's Office and to renew their registration annually.

2.3 The person responsible for records management within the Trust will give guidance for good records management practice and will promote compliance with this policy so that the information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this policy, surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.4 The person responsible is **Rachel Ure, Data Protection Officer**

2.5 Individual staff and employees must ensure that the records for which they are responsible are accurate and are maintained and disposed of in accordance with the school's records management guidelines. This will form part of staff induction procedures.

3 Procedures and practice

3.1 The school follows the guidance as outlined in the 'Information Management Toolkit for Schools' (Version 5 – February 2016) and the guidance of the ICO

3.2 The following practices will be applied within the school:

- The amount of data held should be reduced to a minimum.
- Data held by the school must be routinely assessed to consider whether it still needs to be kept or not.
- Personal data held will be securely stored and sent by secure means.
- The Trust follows the guidance for the information sharing in the case of children subject to safeguarding procedures as set out in 'Information Sharing: Advice for practitioners providing safeguarding services to children, young people, parents and carers' (DfE March 2015) (Appendix E)

4 Auditing

4.1 The Trust must be aware of **all** the sensitive data it holds, be it electronic or paper.

- How long these documents need to be kept will be assessed using the Records Management Toolkit.

- Audits will take place annually.

5 Risk assessment

5.1 If it has not already been undertaken, the Trust will carry out a risk assessment to establish what security measures are already in place and whether or not they are the most appropriate and cost effective available.

5.2 Carrying out a risk assessment will generally involve answering the following questions:

- How sensitive is the data?
- What is the likelihood of it falling into the wrong hands?
- What would be the impact of the above?
- Does anything further need to be done to reduce the likelihood?

5.3 Once the risk assessment has been completed, the school can decide how to reduce any risks or whether they are at an acceptable level.

5.4 Risk assessment will be an on-going process and the school will have to carry out assessments at regular intervals as risks change over time.

6 Securing and handling data held by the school

6.1 The Trust will encrypt[2] any data that is determined to be personal or commercially sensitive in nature. This includes fixed computers, laptops and memory sticks.

6.2 Staff should **not** remove or copy sensitive data from the organisation or authorised premises unless the media is:

- encrypted,
- is transported securely
- will be stored in a secure location.

6.3 This type of data should not be transmitted in unsecured emails (e.g. pupil names and addresses, performance reviews etc).

6.4 Internal exchange of data should be done via email or paper, providing a link to the location of data on the secure server. Alternatively, data transfer should be through a secure encrypted email system e.g. S2S, SecureNet Plus, common transfer files and school census data. If this is not available then the file must be minimally password protected or preferably encrypted before sending via email, the password must be sent by other means and on no account included in the same email. A record of the email should be kept, to identify when and to whom the email was sent, (e.g. by copying and pasting the email into a Word document). Never put personal information such as pupils' names in the subject line of any email.

6.5 Data (pupil records, SEN data, contact details, assessment information) will be backed up, encrypted and stored in a secure place – e.g. safe / fire safe / remote backup.

6.6 All staff computers will be used in accordance with the Teacher Laptop Policy that forms part of the Trust's Code of Conduct.

6.7 When laptops are passed on or re-issued, data will be securely wiped from any hard drive before the next person uses it (not simply deleted). This will be done by a technician using a recognised tool, e.g. McAfee Shredder.

6.8 The Trust's wireless network (WiFi) will be secure at all times[3].

6.9 The Trust will identify which members of staff are responsible for data protection and will ensure that staff who are responsible for sets of information, such as SEN, medical, vulnerable learners, management data etc. know what data is held, who has access

[2] Encryption of computers and memory sticks can be provided by the school's technical support. Guidance is available from http://schools.becta.org.uk/index.php?section=lv&catcode=ss_lv_mis_im03&rid=14734

[3] The school will use WPA2 (or WPA if WPA2 is not available). The older standard WEP will not be used.

to it, how it is retained and disposed of. Appendix B details which members of staff are responsible for which data. This is shared with all staff concerned within the school.

6.10 Where a member of the school has access to data remotely (e.g. SIMS from home), remote access off the school site to any personal data should be over an encrypted connection (e.g. VPN) protected by a username/ID and password. **This information must not be stored on a personal (home) computer.**

6.11 Members of staff (e.g. SMT members) who are given full, unrestricted access to an organisation's management information system should do so as above but need to be aware that higher grades of sensitive data are accessible. **This information must not be stored on a personal (home) computer.**

6.12 The Trust will keep necessary pupil and staff information in accordance with the Records Management Society's guidance.

6.13 The Trust should securely delete commercially sensitive or personal data when it is no longer required as per the Records Management Society's guidance.

6.14 All staff will be trained to understand the need to handle data securely and the responsibilities incumbent on them, this will be the responsibility of the Principal. Completion of this training by all appropriate members of Trust staff is mandatory and details of the date on which the training was completed will be held.

References:
The Data Protection Act 1998:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Information Commissioner's Office
https://ico.org.uk/for-organisations/education/