Salisbury Plain
Academies

Data Protection Policy

Salisbury Plain Academies. CEO: Helen Mathieson.
Bulford St Leonards, John French Way, Bulford, Salisbury, Wilts, SP4 9HP
Registered in England: 10163646, Avon Valley College, SP4 8HH

SALISBURY PLAIN ACADEMIES POLICIES

VERSION CONTROL SHEET

POLICY NAME: Data Protection

Policy Prepared by: Janice Wright, HR Adviser

Document date	Filename	Mtg submitted	Summary of changes required
Feb 2017		FAME 08/03/2017	

Policy Review Date

Contents

1 INTRODUCTION 4

2 DATA PROTECTION OFFICER 4

3 DEFINITIONS 5

4 THE DATA PROTECTION ACT 5

5 EXAMPLES OF DATA 5

6 HANDLING AND RETENTION OF RECORDS 6

7 ACCESS TO PERSONAL INFORMATION 6

8 DISCLOSURE OF PERSONAL INFORMATION 7

9 RETENTION OF RECORDS 7

10 MONITORING OF EMAIL AND INTERNET COMMUNICATION 8

11 DISCIPLINARY ACTION 8

DATA PROTECTION POLICY

This policy is applicable to all students, staff and parents of Salisbury Plain Academies

This policy should be read in conjunction with the following:

Data Protection Act	Jul 1998
E-Safety Policy	
Freedom of Information Act	Nov 2000
Safeguarding and Child Protection Policy	
Safer Recruitment and Selection Policy	
Transfer of Undertakings (Protection of Employment) Regulations	Feb 2006
IT Acceptable Use Policy	
Freedom of Information Policy	July 2016

1 Introduction

1.1 Salisbury Plain Academies ("SPA") will hold and process confidential, personal and sensitive personal information about people, such as names and addresses of staff and students, families, health and other private matters.

1.2 This policy is designed to assist in the avoidance of a breach of the Data Protection Act 1998 ("DPA"), which provides strict rules in this area.

1.3 This policy is designed to be used by, senior staff, HR, line managers, teaching and support staff and administrative staff within SPA and its Board of Directors and members of the local advisory board.

1.4 Please also refer to SPA's Freedom of Information Policy and E-Safety Policy.

2 Data Protection Officer

2.1 SPA's Data Protection Officer is the Director of Business and Finance.

2.2 If you are in any doubt about what you may or may not do, seek advice from SPA's Data Protection Officer.

3 Definitions

3.1 "Personal Data": Personal data is information relating to a living individual who can be identified from those data or from those data and other information which is or might become available to anyone in SPA, or anyone we do business with.

3.2 "Sensitive Personal Data": Some personal data is classed as sensitive personal data. This type of data is subject to further regulations under the Data Protection Act and can only be processed under certain circumstances.

Personal data becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- racial or ethnic origin;
- political opinions;
- religious beliefs;
- trade union membership;
- physical or mental health;
- sexual life;
- committing of offences or alleged offences.

4 The Data Protection Act

4.1 The Data Protection Act 1998 requires that eight data protection principles be followed in the handling of personal data. These are that personal data must:

- be fairly and lawfully processed;
- be processed for limited purposes and not in any manner incompatible with those purposes;
- be adequate, relevant and not excessive;
- be accurate;
- not be kept for longer than is necessary;
- be processed in accordance with individuals' rights;
- be secure; and
- not be transferred to countries without adequate protection.

5 Examples of Data

5.1 The following are examples of personal data and sensitive personal data kept by SPA on members of staff:

- Full name
- Home address
- Home or contact telephone number
- National Insurance Number
- Bank account details (where appropriate)

5.2 During an employee's service other personal information about them is accumulated including:

- Employment application form, Curriculum Vitae and references
- Sickness records
- Annual, special, unpaid and compassionate leave records
- Personal appraisal and assessment records
- Training records
- Disciplinary records
- Promotion and transfer records
- Accident and injury at work records

Data includes both paper and electronic records.

These lists are not exhaustive and items can be added or deleted at any time.

6 Handling and Retention of Records

6.1 When handling and retaining personal information about its employees SPA undertakes to:

- Respect the privacy and human dignity of all employees
- Limit intrusions of any kind to reasonable actions in circumstances where they can be justified
- As far a possible obtain personal data from the employee concerned on the basis of "informed consent"
- Minimise the amount of personal data held throughout SPA
- Collect personal data only for justified reasons, e.g. emergency contact
- Control access of personal data so it is strictly "need to know" basis
- Ensure that all personal data processed by third parties e.g. Payroll / Occupational Health Provider is carried out to SPA's own standard
- Inform employees joining SPA that you hold personal data about them on file and the purpose of holding that data. Also advise them of their rights under the Act
- Ensure that the disclosure of personal data to third parties is only made after written authorisation from the employee has been received. Record all disclosures made to third parties in terms of who made the request, which data was disclosed and the time and date of the disclosure

7 Access to Personal Information

7.1 An individual employee has certain rights under the DPA with regard to the information held about them. These are:

- The right to access to the information held about them
- The right to know that the company is processing the information, what information is being processed, why it is being processed and to whom it may be disclosed
- The right to prevent direct marketing using the information held about them
- The right to have personal information corrected
- The right to compensation if they are affected by errors in the information held
- The right to prevent automated decisions being made by a computer based upon the information held

7.2 An individual has the right to view the data held by SPA about them and to amend it at any time when their personal circumstances change.

8 Disclosure of Personal Information

8.1 The personal information held by SPA about employees will only be disclosed to those within the company who are authorised to have access to it and only then if that disclosure is directly connected to their normal duties.

8.2 The following staff are authorised to have access to employee personal information:

- Chief Executive Officer /Principal, Operations Officer and CEO's Personal Assistant – all information
- Member(s) of Human Resources dealing with personal matters – all information
- Line managers – leave, appraisal and training information only
- SPA's Occupational Health advisers – information only applicable to the Occupational Health matter being discussed.

8.3 Personal information held by SPA may also be disclosed to outside agencies such as the Police and HM Revenue and Customs, but such disclosure is only made under certain circumstances defined in the DPA.

8.4 In the event that the Transfer of Undertakings (Protection of Employment) Regulations 2006 apply so far as is possible data will be supplied in an anonymous form and if that is not possible, then the prospective employer will be required to keep such information confidential. The employee to whom the information refers is to be informed of the nature and means of such a disclosure.

8.5 The internal transmittal of personal information between authorised members of staff must be made in such a way that the information cannot be seen by those who are not authorised to see it. As a general rule this should be by means of a properly marked sealed envelope. Where this is not possible or impractical and personal information is to be transmitted by fax or e-mail, the following precautions must be taken:

- The transmittal of personal information should only be made over a secure network or by comparable means, or if e-mail is used, then by encryption.
- Where transmittal is made by fax, the transmittal is to be made by prior arrangement and the assigned recipient is to personally monitor the arrival of the fax at its destination.
- All copies of faxes or e-mails held by both senders and recipients are to be retained securely.
- Senders and recipients are responsible for ensuring that e-mails containing personal information about employees are deleted from the e-mail accounts at the earliest opportunity.

9 Retention of Records

9.1 It is necessary for a number of statutory reasons or for reasons of continuity, that SPA must retain a certain amount of personal information about current and former employees. The following information is recommended by the Information

Commissioner in its Employment Practices Data Protection Code for periods which information is to be retained. This is shown in the following table:

Application form & selection documentation (unsuccessful applicant)	Six months
Application form (employee)	Duration of employment
References received	Duration of employment
Payroll and tax information	6 years
Sickness records	3 years
Annual leave records	2 years
Unpaid leave/special leave records	3 years
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
References given/information to enable references to be provided	5 years from reference/end of employment
Summary of record of service, e.g. name, position held, dates of employment	10 years from end of employment
Records relating to accident or injury at work	12 years

Any data protection queries should be addressed to the Data Protection Officer.

10 Monitoring of Email and Internet Communication

10.1 SPA monitors e-mails and internet communications and activity. Further information can be found in the IT Acceptable Use Policy.

11 Disciplinary Action

11.1 The access to personal information about an employee by any member of staff who is not authorised to do so will be treated as a matter of gross misconduct and will be subject to disciplinary action. Such access is also a criminal offence under the DPA.

11.2 The unauthorised disclosure of personal information about an employee to any person not authorised to receive it will be treated as a matter of gross misconduct on the part of the person disclosing the information and the person receiving it, and will be subject to disciplinary action.