Sandwell Academy Data Protection

Policy Title:	Data Protection
Policy Reference:	SA / IT
Description:	This document sets out the Academy's responsibilities under the Data Protection Act 1998.
Status:	Statutory
Category:	Academy
Contact:	Name: Mr K Hull Title: Deputy Head Email : Khull@sandwellacademy.com
Version:	V1.1
Other relevant TOA polices:	None
Adopted by the Governing Board on:	
Date for Review:	July 2019

Change Record		
Version	**Date**	**Description**
1.1		
1.2		
1.3		
1.4		

Contents Page

Table of Contents

INTRODUCTION

All records and data are confidential documents for use only within and by the Academy for matters relating to individual members of staff and students. All staff need to maintain and respect an individual's right to privacy and in doing so should be careful not to disclose personal information that could compromise the individual concerned or themselves. This policy document will contain procedural advice taken from 'General Data Protection Regulations (2018) relating to the use of data in the employer/employee relationship following the Data Protection Act 2018. All references to the handling and management of student data are to be found in Student Records Policy.

What is the point of the GDPR?

The GDPR and new DPA exist to look after individual's data. It is a series of safeguards for every individual. Information about individuals needs to be treated with respect and be secure. The GDPR exists to protect individual rights in an increasingly digital world.

The Six Key Principles of GDPR

Lawfulness, transparency and fairness.	School's must have a legitimate reason to hold the data, and need to tell people what data school collects and how it is used.
Collect data for a specific purpose and use it for that purpose.	So, data cannot be used for a purpose that it was not originally collected for, or where notice has not been given about how data may be used after collection.
Limited collection	Data controllers should only collect the minimum amount of data needed for a particular task or reason. If there is a breach or a hack only limited information can be lost.
Accuracy	Data collected should be accurate, and steps should be taken to check and confirm accuracy.
Retention	There must be a policy that requires data to be stored for limited periods about individuals. Data should not be stored for longer than it is needed, or for historical archive reasons.
Security	Ensuring that physical, cloud and other electronic storage of data is secure is vitally important. Everyone has a responsibility for the data they hold and process. This also includes third party contractors

PERSONAL INFORMATION DATA

All staff are data subjects and both manual and electronic data relating to individuals is to be managed in accordance with the Data Protection Act 1998. The Sandwell Academy Trust Limited is the Data Controller and is registered with the Information Commissioner. The register entry describes in general terms, the personal data being processed by the Academy and the purposes for processing. The Data Controller is legally liable for implementing the Data Protection Act 1998 and the implementation of this policy.

The register entry describes in general terms the personal data being processed by the Academy for five purposes:

1. Education
2. Educational Support and Ancillary Purposes
3. Schools Administration
4. Staff, Agent and Contractor Administration
5. Advertising, Marketing, Public Relations, General Advice Services

The Data Protection Policy covers the following Data Subjects for the five purposes:

- Applicants (successful and unsuccessful)
- Former applicants (successful and unsuccessful)
- Employees (current and former)
- Advisors, consultants and agency workers (current and former)
- Casual workers (current and former)
- Volunteers (current and former)
- Work experience workers (current and former)
- Suppliers (current and former)
- Contract workers (current and former)
- Complainants, correspondents and enquirers (current and former)
- Relatives/Guardians (current and former)
- Governors (current and former)
- Health professionals (current and former)
- Welfare and pastoral professionals and advisors (current and former)
- Business and other contacts (current and former)
- Previous and prospective employers, referees
- Authors, publishers, editors, artists and other creators (current and former)

The areas covered by the Data Protection Policy relate to one or more of the five purposes and include:

- Personal details
- Family, lifestyle and social circumstances
- Education and training details
- Employment details
- Financial details
- Racial or ethnic origin
- Religious or other beliefs of a similar nature
- Physical or mental health or condition
- Student records
- Disciplinary records

- Sexual orientation
- Offences (including alleged offences)
- Goods or services provided
- Trade Union membership
- Lifestyle and social circumstances

For further information refer to the Register Entry (available upon request).

Personal data includes information that relates to a living person. It is information that identifies an individual either on its own or together with other information that is in the organisation's possession currently or in the future.

Any form of personal data that is filed, electronically stored or processed is covered by the Data Protection Act 1998 and the Data Controller will observe the rights of individuals within the legal requirements of the Act. Only data that is of specific relevance and importance will be required by the Data Controller, who will ensure that the data is securely stored to maintain an individuals' right of privacy. Personal information data will only be shared with relevant personnel or individuals from related agencies or organisations.

SENSITIVE PERSONAL DATA

Sensitive personal data are information concerning an individual's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership
- Physical or mental health
- Sexual orientation
- Commission or alleged commission of any offence
- 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

Sensitive personal data found in an individual's record might typically be about their:

- Physical or mental health – as part of sickness records
- Disabilities – to facilitate adaptations to the Academy
- Racial origin – to ensure equality of opportunity
- Trade union membership – to enable deduction of subscriptions from payroll

In the context of staff recruitment and selection typical circumstances in which sensitive personal data might be requested and held include:

- Relevant criminal convictions to assess suitability for employment
- Disabilities to ensure special needs are catered for at interview
- Racial origin to ensure recruitment processes do not discriminate against ethnicity

The collection and processing of sensitive personal data should only be done when the data subject has given explicit consent to the processing.

THE ROLE OF THE DATA CONTROLLER

Sandwell Academy Trust Limited is the legally appointed Data Controller. The designated Data Controller within the Academy with respect to managing the Data Protection Policy is the Headteacher.

Responsibilities include:

- Overview of what personal data are processed.
- Ensuring employment practices are compliant with the Data Protection Act 1998.
- Checking and evaluating procedures in place.
- Ensuring that all individual line managers that process information understand their own responsibility for data protection compliance and if necessary amend their working practices.
- Assessing what personal data is in existence and who is responsible for them.
- Maintaining a complete inventory of personal data held in electronic and manual form.
- Eliminating the collection of personal data that are irrelevant or excessive.
- Ensuring that a sensitive personal data condition is satisfied.
- Ensuring that individuals are aware of the extent to which they can be criminally liable if they knowingly or recklessly disclose personal data outside the Academy's procedures and policies. Making serious breaches of data protection rules a disciplinary offence.
- Ensuring that the Academy has a valid notification in the register of data controllers and it is up to date.
- Consulting trade unions, other workers' representatives or workers themselves over the development and implementation of employment practices and procedures that involve the processing of workers' data.
- Responding to the Data Protection Commissioner in a co-operative way to all enquiries.

THE MANAGEMENT OF PERSONAL DATA ABOUT EMPLOYEES

Sandwell Academy will strictly control access to any human resource records at all times, a formal 'need to know' basis will be observed. The dignity and privacy of all employees will be respected.

Personal data will be held in different formats. Electronic data will be stored in a secure environment. Manual personal data information will be held on file in locked cabinets in a restricted area of the Academy. All personal data information will be under the due restriction of the Data Controller.

Employees will be informed annually that personal data relating to them is being held by the Academy, this will be done in written form at the advice of the Data Controller. The employee will check the information is correct and notify the Data Controller of any errors. The details that should be given are:

- The sources of personal data
- The types, or categories, of data
- The parties who have access to that data

- The precise purpose(s) for holding the data
- If they are the subject of automated decisions
- Their individual rights to access files and rectify, erase or block data that is incomplete or inaccurate.

Employees have a right to gain a copy of all personal data about themselves the process being outlined under the section 'The Rights of Data Subjects'. The rights outlined in this section should be managed as detailed.

If any employee would be unlikely to comprehend the meaning of any information held on the files that they have requested, a written explanation must be provided by the Data Controller.

The disclosure of all personal data to third parties should either be on the basis of a statutory right or after obtaining the prior, explicit consent of the employee concerned. No personal data will be released to a third party until their identity has been carefully verified. All such disclosures should be logged by reference to the party making the request, the time and date when the request was satisfied. Where the Data Controller becomes aware that disclosure requests may involve fraudulent behaviour, the employee concerned should be informed and encouraged to contact the Police.

If personal data is processed by a third party on behalf of the Academy, the relationship between the two parties will be subject to a written contract. This will state that the third party must process that data only within the terms of the instructions issued by the Academy.

No personal data should be processed in any form that may give rise to the substantial damage, distress or detriment to any employee or any other individual identified by that data. If a notice in writing is made by an employee to prevent such processing the Data Controller will respond within twenty-one days stating:

- How the Data Controller intends to comply with the notice, or
- Giving reasons why full compliance would not be justified.

If refused an employee then may seek legal redress through the courts.

The Data Controller will obtain explicit consent from the employee before transferring personal data about them to countries outside the European Union, Norway, Iceland and Liechtenstein. No staging posts other than the aforementioned should be used to transfer personal data to a third country. No non-encrypted e-mails containing personal data will be transmitted via the Internet.

THE RIGHTS OF DATA SUBJECTS

Data Subjects are entitled to be informed by the Data Controller whether personal data relating to them are being processed by or on behalf of the Data Controller. The data that can be given by the Data Controller to the Data Subject can be:

- The personal data of which that individual is the Data Subject
- The purposes for which they are being or are to be processed
- The recipients or classes of recipients to whom they are or may be disclosed
- The personal data that relates to the Data Subject's performance at work, creditworthiness, reliability or conduct that has constituted or is likely to constitute the sole basis for any decision significantly affecting them, to be informed of the logic involved in the decision-taking.

Data Subjects have a right to have a copy of the information that the Academy holds about them. The formal process being:

- The Data Subject makes a written request and signs it to verify personal identity (in some instances a fee may be requested).
- The Data Controller must be sure of the identity of the Data Subject making the request.
- The Data Controller must respond to the request once satisfied of the identity being satisfied.
- The Data Controller must communicate the information requested in an intelligible form. This may include information constituting any personal data of which the individual is the Data Subject and any information available to the Data Controller as to the source of those data.
- The Data Controller must make the relevant particulars available promptly, and if practicable on the same day as the written request up to forty days after the request is received, unless the Data Controller is unable to comply with the request.

The Data Controller cannot comply with a request if the information requested relates to another individual who can be identified from that information. The request can only be met if the other individual has consented to the disclosure of the information to the person making the request or if the Data Controller believes the circumstances negate the need to seek consent of the other individual. In such instances the Data Controller will consider:

- Any duty of confidentiality owed the other individual
- Any steps taken by the Data Controller with a view to seeking the consent of the other individual
- Whether the other individual is capable of giving consent
- Any express refusal of consent by the other individual

If the Data Subject believes that the information held about them by the Academy is inaccurate, they should notify the Data Controller, they may also apply to the courts to obtain an order requiring the Data Controller to correct any inaccuracies. In such instances the Data Subject may seek compensation where damage or distress have been caused as a result.

Individuals may also object to the processing of personal data about them and the Data Controller must respect this right unless it prejudices the detection of crime or the apprehension of offenders. The Data Controller must respond within twenty-one days following such a request from the Data Subject.

RECRUITMENT

Sandwell Academy will provide applicants with a clear description of the job it is seeking to fill. The application form will seek to gain personal information that is relevant to the position to be filled within the environment of an academic institution.

Candidates will be informed about:

- The purposes for which the Academy is collecting the information
- How long the Academy intends to keep the information
- The security safeguards in place to protect information
- Who will have access to the information

- How the application will be processed

The Academy will gain explicit consent from candidates to hold personal data about themselves through the application form. All candidates will be informed in advance that the Academy may verify the information contained in their application gaining written consent again through the application form for:

- The Academy to carry out the verification process
- Relevant third parties to release personal information about them in connection with the current vacancy

Personal data that are recorded as part of the selection process will be retained following interview and filed. Candidates have a right to see any notes made during the interview process and will be informed that the information will be kept for a period of six months. Candidates will be asked if they wish their names to remain on file for future vacancies and will be given the opportunity to have their details removed from the file. All data will be securely stored.

The Academy will review biannually, all files relating to previous job applications. Files will be kept for a period of six months then removed and securely destroyed.

All applicants will be required to fill in a Monitoring Form that will be used to provide a database to monitor the age and ethnicity of all applicants and not as part of the selection process.

Sandwell Academy is registered with the Disclosure and Barring Service. Successful applicants will be screened following appointment on condition of not having a criminal conviction that would compromise the safety and well being of staff or students. An offer of employment will be upheld in the light of a positive screening. For further information regarding the Disclosure and Barring Service refer to the ‘Code of Practice and Explanatory Guide for Registered Persons and other recipients of Disclosure Information’.

Appendix One – Guidelines for staff who have access to personal data

What is personal data?

"Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context."

" Anything that can identify an individual."

Personal Descriptors: Name, age, place of birth, date of birth, gender, weight, height, eye color, hair color, fingerprint

Identification Numbers : Health IDs, Social Insurance Numbers (SIN), Social Security Numbers (SSN), PIN numbers, debit and credit card numbers

Ethnicity : Race, colour, national or ethnic origin

Health : Physical or mental disabilities, family or individual health history, health records, blood type, DNA code, prescriptions

Financial :Income, loan records, transactions, purchases and spending habits

Employment : Employee files, employment history, evaluations, reference interviews, disciplinary actions

Credit : Credit records, credit worthiness, credit standing, credit capacity

Criminal : Convictions, charges, pardons

Life : Character, general reputation, personal characteristics, social status, marital status, religion, political affiliations and beliefs, opinions, comments, intentions

Education : Education history

What are the Academy's preferred methods of accessing personal data?

1. Through PCs based at the Academy site.
2. Through the use of Virtual Office when you are not based at the Academy site.

It is not an acceptable reason for employees to say that they can't access Virtual Office or they cannot 'make it work'. The IT team are happy to support employees in their access of Virtual Office.

3. Through an encrypted USB drive purchased from the IT team at Sandwell Academy. The Academy recognises that on occasions, documents such as IEPs are not accessible via Virtual Office. However, Virtual Office should be the second preferred method and staff who wish to purchase an encrypted USB drive will need to demonstrate a need for the device.

What type of access to personal data is completely unacceptable?

1. Access to personal data through a PC or device in a public place. Eg Library or Coffee shop WIFI hotspot.
2. Access to personal data through an unencrypted USB drive through a public PC or a PC at home and then the storage of personal data on these types of devices.

Mobile Phones

Employees who are provided a work mobile phone must ensure that their phone has a PIN number to allow access.

Employees who have chosen to receive their work email to a personal mobile phone must ensure that their phone has a PIN number to allow access. Employees are not allowed to access work email through a personal mobile phone which is not protected by a PIN number.

As at June 2013, the IT Director is trialling software which monitors this requirement and will speak to any employees who breach this expectation.

Data Protection Agreement – for staff who require an encrypted USB drive

This Agreement is dated the ……. day of …… 20……., made between Sandwell Academy Trust ("the Employer") and ……. ("the Employee")

IT IS HEREBY AGREED AS FOLLOWS:

The Employee understands his / her responsibilities under the Data Protection Act 1998 and confirms that s/he has been issued with an encrypted USB device by Sandwell Academy.

The Employee agrees that any information which is moved by electronic means from Sandwell Academy must be saved to this encrypted device only.

The Employee agrees that any personal information sent by electronic means externally must be password protected.

The Employee agrees that s/he will not use any other USB device which is not encrypted to save electronic information, this includes the saving of information to their PC / Mac at home.

The Employee understands that the loss of the encrypted USB device must be reported to the Director for IT as soon as possible.

This agreement remains in force during the employment term of the Employee and the USB device will be returned to the Director for IT at the end of the employment.

Signed _____

(Employee)

Dated _____

Signed _____

(For and on behalf of Sandwell Academy Trust)

Dated _____