Windhill Academy Trust

Data Security Policy

June 2018 v2

Policy Review Information

Version	Reason for review	Approved by	Date approved
2	Following audit by Data Protection Officer on 21/6/18	Resources Committee	26/6/2018

Contents

Section Title	Page No.
Part 1 – Introduction & Key Definitions	
Introduction	4
Key Definitions	4
Part 2 – Organisational Arrangements	
Overall Responsibility	6
Roles & Responsibilities	6
Part 3 – Detailed Arrangements & Procedures	
Data Management • Data Registration • Data Protection Officer • Data Protection Awareness • Data Mapping	6
Third Party Suppliers Acting as Data Processors	9
Consent • Privacy Notices • The Use of Pupil Images • Accurate Data • Withdrawal of Consent	10
Associated Data Protection Policies and Guidance re: • CCTV • Complaints • Data Breaches • Records Management & Retention • Subject Access Requests • Third Party Requests for Information • Use of Personal Devices	11

Part 1 Introduction and Key Definitions

1.1 Introduction

Windhill Academy Trust needs to gather and use certain information about individuals. These individuals can include pupils, parents/carers, employees, suppliers, business contacts and other people the academy has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the academy's data protection standards and to comply with the law.

This data protection policy ensures that Windhill Academy Trust:

- complies with data protection law and follows good practice;
- protects the rights of pupils, staff, parents/carers and other stakeholders;
- is open about how it stores and processes individuals' data and
- protects itself from the risks of a data breach.

This Data Security Policy is based on the six principles of the Data Protection Act (DPA) that personal data shall be:

1. processed lawfully, fairly and in a transparent manner;
2. collected for specified, explicit and legitimate purposes;
3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
4. accurate and kept up to date;
5. kept in a form which permits identification of data subjects for no longer than is necessary;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss or damage;

1.2 Key Definitions

Data

The DPA describes how organisations, including Windhill Academy Trust must collect, handle and store personal information ('data').

Data is any information that the school collects and stores about individuals or organisations. Some data is more sensitive than others and particular care will be given to processing and managing this. Sensitive data includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data concerning health or sex life and sexual orientation;
- genetic data; and
- biometric data.

Data can be stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Data Subject
A 'Data Subject' is someone whose details the academy keeps on file. The data subject has the following rights under data protection legislation:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Although data protection legislation affords these rights to individuals, in some cases the obligations schools have to share data with the DfE etc. override these rights (this is documented later in the policy under 'Privacy Notices').

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location number, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller
The 'Data Controller' has overall responsibility for the personal data collected and processed and has a responsibility for ensuring compliance with the relevant legislation. They are able to delegate this to 'Data Processors' to act on their behalf. The Academy Trust is the 'Data Controller'.

Data Processor
A 'Data Processor' uses, collects, accesses or amends the data that the controller is authorised to collect or has already collected. It can be a member of staff, third party company or another organisation such as the police or Local Authority (LA).

Part 2 Organisational Arrangements

2.1 Overall Responsibility

Windhill Academy Trust will meet its obligations under the DPA by putting in place clear policies that focus on the key risks and in checking that control measures have been implemented and remain appropriate and effective.

2.2 Roles & Responsibilities

The Governing Body will:

- Establish and maintain a positive data protection culture;
- Ensure the Headteacher prepares a Data Security Policy for approval and adoption by the Governing Body and to review and monitor the effectiveness of the policy;
- Appoint a Data Protection Officer and provide adequate resources and support for them to fulfil their statutory duties;
- Allocate sufficient resources for data protection, e.g. in respect of training for staff, encryption technology for devices;
- Monitor and review data protection issues;
- Ensure that the academy provides adequate training, information, instruction, induction and supervision to enable everyone to comply with their data protection responsibilities;
- Review and act upon data protection compliance reports from the Data Protection Officer.

The Headteacher will:

- Promote a positive data protection culture;
- Prepare a Data Security Policy for approval by the Governing Body, revise as necessary and review on a regular basis, at least every two years;
- Ensure that all staff adhere to the policy;
- Ensure that staff are competent to undertake the tasks required of them and have been provided with appropriate training;
- Provide staff with equipment and resources to enable them to protect the data that they are processing;
- Ensure that those who have delegated responsibilities are competent, their responsibilities are clearly defined, and they have received appropriate training;
- Monitor the work of the Data Protection Officer to ensure they are fulfilling their responsibilities;
- Encourage the use of work bags for transporting data.

The Data Protection Officer will:

- Inform and advise the academy of their obligations under data protection legislation;
- Monitor compliance with the legislation and report to the Headteacher and Governing Body on a termly basis;
- Co-operate with the supervisory authority (e.g. Information Commissioner's Office) and act as the main contact point for any issues;
- Seek advice from other organisations or professionals, such as the Information Commissioner's Office as and when necessary;
- Keep up to date with new developments in data protection issues for schools;

- Act upon information and advice on data protection and circulate to staff and governors;
- Carry out a data protection induction for all staff and keep records of that induction;
- Co-ordinate the school response to a Subject Access Request;
- Co-ordinate the school response to a data breach.

Staff at the school will:

- Familiarise themselves and comply with the Data Security Policy;
- Comply with the academy's data protection arrangements;
- Follow the data breach reporting process;
- Attend data protection training as organised by the school;

Part 3 Detailed Arrangements & Procedures

3.1 Data Management

Data Registration
As Data Controller, the school must register as a Data Controller on the Data Protection Register held by the Information Commissioner. The school was last registered on 26/5/2015 and is due to renew on 25/5/2018.

Data Protection Officer
As a public body, Windhill Academy Trust is required to appoint a Data Protection Officer (DPO).

At Windhill Academy Trust, the DPO role is fulfilled by:

Daniel Rowe
dpo@windhill.herts.sch.uk

The role of the DPO is to:

- Inform and advise the school/academy and the employees about obligations to comply with all relevant data protection laws;
- Monitor compliance with the relevant data protection laws;
- Be the first point of contact for supervisory authorities.

Data Protection Awareness
In order to ensure organisational compliance, all staff and other key stakeholders (e.g. governors, volunteers) will be made aware of their responsibilities under the data protection legislation as part of their induction programme, (both as a new employee/governor to the organisation or if an individual changes role within the academy).

Annual data protection refresher training will take place to reinforce the importance of staff adhering to the legislation.

A record of the professional development undertaken by the individual will be retained on their training record.

Data Mapping
Windhill Academy Trust documents all of the data that it collects within a 'Data Flow Map'. This data inventory records:

- the data held;
- what the data is used for;
- how it is collected;
- how consent is obtained;
- how the data is stored;
- details of the retention period;
- who can access the data;
- who is accountable for the data;
- how the data is shared and
- how the data is destroyed.

For each data type, the probability of a data breach occurring is assessed (very high, high, medium, low or very low) and actions to be taken to mitigate the risk are recorded.

It is the responsibility of the DPO to ensure the 'Data Flow Map' is kept up to date. The map is a live document and updated regularly.

3.2 Third Party Suppliers Acting as Data Processors

As Data Controller, the academy is responsible for ensuring that correct protocols and agreements are in place to ensure that personal data is processed by all sub-contractors and other third parties in line with the principles of the data protection legislation.

Individuals within school who have a responsibility for securing contracts and agreements with such third parties are responsible for ensuring that all external data processing is contracted out in line with the principles of the DPA. These type of agreements include:-

- IT contracts and processes.
- Physical data and hard copy documents.
- Data destruction and hardware renewal and recycling financial and personnel information.
- Pupil and staff records.

Only third party suppliers who can confirm they have appropriate technical, physical and organisational security to securely process data will be considered as suitable partners.

The procurement process will ensure that all contracts are suitable and reflect DPA requirements. Review of current and due consideration of future contracts will require this even if data processing is ancillary to the main purpose of the contract.

The external processor will confirm with the data controller that suitable security and operational measures are in place.

Any potential supplier or purchaser outside the EU will be obliged to confirm how they comply with the DPA and give contractual assurances.

The DPO may require a specific risk assessment to be undertaken if the data is sensitive, and if an increased risk is likely due to the nature, or proposed nature, of the processing.

A written agreement will be in place between the supplier and the school to confirm compliance with the DPA principles and obligations to assist the school in the event of data breach or subject access request, or enquiries from the ICO.

The school must have the right conduct audits or have information about audits that have taken place in respect of the relevant processes of the supplier's security arrangements whilst the contract is in place, or whilst the supplier continues to have personal data that relates to the contract on its systems.

Any subcontracting must only be done with the written consent of the school as data controller. This must be the case for any further subcontracting down the chain. All subcontractors must confirm agreement to be bound by DPA principles when handling the school's data, which shall also include co-operation and eventual secure destruction or return of data.

3.3 Consent

As an academy, we will seek consent from staff, volunteers, young people, parents and carers to collect and process their data. We will be clear about our reasons for requesting the data and how we will use it. There are contractual, statutory and regulatory occasions when consent is not required. However, in most cases, data will only be processed if explicit consent has been obtained.

Consent is defined by the DPA as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

We may seek consent from young people also, and this will be dependent on the child and the reason for processing.

Privacy Notices
In order to comply with the fair processing requirements of the DPA, the school will inform their staff and parents/carers of all pupils of the data they collect, process and hold on them, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom their data may be passed, through the use of 'Privacy Notices'.

Privacy notices are available to staff and parents through the following means:

- School website
- School newsletter
- School prospectus
- Electronic communication to parents and staff
- Staff Handbook

The Use of Pupil Images
Occasionally the academy may take photographs of its pupils. These images could be used as part of internal displays, printed publications, the school website or our social media accounts.

The academy will seek consent from all parents to allow the photography of pupils and the subsequent reproduction of these images. Parental consents are valid for the period that their child is on roll at Windhill21 and can be withdrawn by parents at any time. Parents may withdraw any consent(s) by providing the school with written confirmation specifying which consent(s) they wish to amend.

Parents are given the opportunity to opt in. It is not permissible to assume parents are opting in.

Generic consent for all uses of images is not acceptable; parents must give consent to each medium.

Parents must be given the opportunity to withdraw their consent at any time. This should be given in writing to the school.

Consent will be recorded using secure Excel spreadsheets and/or on the school's management information system (SIMS).

If images of individual pupils are published, then the name of that child will not be used in the accompanying text or caption unless specific consent has been obtained from the parent prior to publication.

The academy parental consent forms will be issued to parents for completion as their child joins the school.

Accurate Data
The school will endeavour to ensure that the data it stores is accurate and up to date. When a pupil or member of staff joins the academy they will be asked to complete a form providing their personal contact information (e.g. name, address, phone number, NI number for staff), next of kin details, emergency contact and other essential information. At this point, the academy will also seek consent to use the information provided for other internal purposes (such as promoting school events, activities and photography).

The school will undertake an annual data collection exercise, where current staff and parents will be asked to check the data that is held about them is correct. This exercise will also provide individuals with the opportunity to review the consent they have given for the academy to use the information held for internal purposes.

Parents/carers and staff are requested to inform the academy when their personal information changes.

Withdrawal of Consent
Consent can be withdrawn, subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent, the school will consider each situation on the merits and within the principles of the DPA, child welfare, protection and safeguarding principles.

Parents/carers and staff are requested to provide the school with written confirmation specifying which consent(s) they wish to amend. This should be returned to the Administrator with responsibility for pupils and data.

3.4 Associated Data Protection Policies and Guidance

- CCTV Policy
- Complaints Procedure
- Data Breaches Policy
- Records management toolkit for schools from the Information and Records Management Society (IRMS).
- Subject Access Requests
- Third Party Requests for Information
- Use of Personal Devices (included in the school's Data Security Policy)

CCTV
Windhill Academy Trust uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to the school property. The academy has a CCTV policy in place which documents:

- why CCTV is used;
- where cameras are sited;
- whether covert monitoring is undertaken;
- retention periods for images held;
- who has access to the images;
- details of the complaints procedure.

Complaints
Complaints will be dealt with in accordance with the academy's Complaints Procedure.

Data Breaches
Although the academy takes measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data as set out in this policy and the supporting policies referred to, a data security breach could still happen. Examples of data breaches include:

- Loss or theft of data or equipment on which data is stored (e.g. losing an unencrypted USB stick, losing an unencrypted mobile phone);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (e.g. sending an email to the wrong recipient, information posted to the wrong address, dropping/leaving documents containing personal data in a public space);
- Unforeseen circumstances such as fire or flood'
- Hacking attack;
- 'Blagging' offences where information is obtained by deceiving the academy trust.

Details of the school policy which sets out the process that should be followed in the event of a data breach occurring is included in the Data Breach Policy.

Privacy Impact Assessments
When considering the purchase of a new service or product that involves processing personal data, a Data Privacy Impact Assessment must be completed by the DPO. If risks are identified as part of the assessment then appropriate steps to mitigate this risk must be implemented. If these risks are deemed to be 'critical risk' then the DPO should consult with the ICO prior to implementation.

The 'Data Privacy Impact Assessment' form must be used for each new service/product.

Records Management
The academy recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations which will also contribute to the effective overall management of the school.

We retain data for the length of time specified by the records management toolkit for schools from the Information and Records Management Society (IRMS). Details of retention periods for different aspects of your personal information are available from http://irms.org.uk/page/SchoolsToolkit.

Subject Access Requests
Any individual, person with parental responsibility or young person with sufficient capacity has the right to ask what data the school/academy holds about them, and can make a Subject Access Request (SAR).

The school's process for managing a Subject Access Request is set out in the school's Subject Access Request policy.

Third Party Requests for Information
Occasionally the academy may receive a request for information on a pupil or member of staff by a third party, such as the police or social services. This would be separate to statutory requests that come through from the DfE or LA, for example, which are covered within the privacy notices.

The academy's Third Party Request for Information policy sets out the process that should be followed in the event of receiving a third party request.

Use of Personal Devices
The academy recognises the benefits of mobile technology and is committed to supporting staff,as detailed in the acceptable use of mobile devices. The academy's acceptable use agreement for staff and governors sets out how non-school owned electronic devices, e.g. laptops, smart phones and tablets, may be used by staff members and visitors to the school.