General Data Protection Regulations (GDPR)

Foxwood Academy Data Protection Policy

Approved June 2019 – Review every 1 years

(June 2020)

Data Protection Policy

Contents

1. Introduction
2. Definitions
3. Policy aim
4. Policy objective
5. Processing of information
6. What counts as personal information
7. Processing of special categories of personal information
8. Access to information
9. Fair Obtaining/Processing
10. Data Uses and Purposes
11. Data Incident Reporting/ Data Breach
12. Data Quality and Retention
13. Records of processing activities
14. Data Security

Data Protection Policy

1. Introduction

Foxwood Academy aims to ensure that personal information is treated lawfully and correctly. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the Academy deals and in achieving its objectives. This policy sets out the basis on which the Academy shall process any personal data from the students, their parents/carers, staff and other parties from whom data is collected.

The Academy, and therefore any person who handles personal data on behalf of the Academy, fully endorses and adheres to the data protection principles set out in Article 5 of the GDPR and sections 83-89 DPA 2018 as below and shall be responsible for and be able to demonstrate compliance with the principles outlined below:-

THE SEVEN DATA PROTECTION PRINCIPLES

Personal Information shall be:

- processed lawfully, fairly and in a transparent manner **(lawfulness, fairness and transparency)**
- collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;**(purpose limitation)**
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**(data minimisation)**
- accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(accuracy)**
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (**storage limitation**)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**)

- kept in a responsible manner and compliance is demonstrated by ensuring there are appropriate measures and records in place along with compliance of all data principles **(accountability)**

2. Definitions

Personal data

Means any information relating to an identified or identifiable natural person (data subject). 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 data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed.

Consent

Means any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.

Special categories of personal data

Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation.

Processing

Includes any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, use, disclosure, erasure or destruction.

Educational records

The right of access to any record of information which relates to a pupil and therefore includes any education, health and care plan and any personal education plan. Educational records do not include information which is processed by a teacher solely for the teacher's own use such as lesson plans.

Subject Access Request

Right to access to the personal data by the pupil or parent/carer of the pupil.

Data subject

This will be the person that we collect the data from. This will include pupils, family members and staff.

3. Policy Aim

To ensure the Academy complies with all relevant legislation and good practice to protect all of the personal information that it holds.

4. Policy Objectives

To achieve the overall aim the Academy will:

- Provide adequate resources to support an effective approach to data protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the Academy's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its staff at all levels to ensure standards are met.
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

5. Processing of Information

The Academy, through appropriate management controls will, when processing personal information about any individual:

Observe fully the conditions regarding the collection and use of information and meet the Academy's legal obligations under the GDPR and the Data Protection Act 2018.

Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

Ensure that the individual about whom information is held can exercise their rights under the Act unless an exemption applies for example in relation to education data, including the right:-

- to be informed that processing is being undertaken
- to prevent processing in certain circumstances
- to correct, rectify, block or erase information, which is regarded as incorrect information
- of access to personal information
- to erasure
- to portability where applicable.

6. What counts as Personal Information?

This is any information held by the Academy about a living individual, from which that individual can be identified. For example, this includes:

- A name and address or contact details held about pupils, parents and staff and their families
- information attached to a reference number that could be used to identify someone
- a pupil's Academy record
- photographs of a child
- records of sickness absence
- financial records relating to a child's parent

7. Processing of special categories of personal Information

The Academy, through appropriate management controls will, when processing special categories of personal information about any individual:

- Observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet the Academy's legal obligations under the GDPR and the Data protection Act 2018. In particular, Schedule 1 Part 4 of the DPA 2018 states that the Academy must have this policy document in place which explains as below, the procedures for securing compliance with the principles in Article 5 as outlined above.
- Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.
- Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs data, data concerning health or data concerning a natural person or trade union membership and the processing of genetic data biometric data for the purpose of uniquely identifying a natural person.

8. Access to Personal Information

The Academy will process requests for access to personal information in line with the relevant sections of the GDPR and the Data Protection Act 2018.

Subject Access Requests

Individuals can request a copy of the personal data the Academy holds about them. Any staff member who receives a valid data protection request must forward it to the Data Protection Officer for the Academy.

- if more information is required this will be requested from the requester;

- if all information has been received, and the request is a valid subject access request, the Academy will acknowledge the request and process the request within one month from receipt; unless the request is particularly large and complex in which case the time can be extended for two months.

Access to educational records

The Education (Pupil Information) (England) Regulations 2005 allow parents access to the official education records of their children. The Academy must make a pupil's educational record available for inspection or provide a copy of the record within 15 days of a valid written request by a parent. Any charges for copying will not exceed the cost of supply.

The Academy may refuse to disclose information under the Pupil Information Regulations where:

- The Academy would have no right to disclose the information to the pupil under the GDPR and DPA 2018.
- This may be where the information might cause serious harm to the physical or mental health of the pupil or another individual.

When providing information to an individual, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Academy staff should disclose information in line with the Academy's Personal Information Request Policy.

The Academy should not disclose anything on a pupil's record that would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those creating such records should make sure this kind of information is kept separate from the pupil's other records. Where there is a doubt or statutory requirements conflict staff should seek advice in the first instance from the Data Protection Officer.

Requests from other agencies for personal information

- Requests from any external agency will be processed in accordance with the GDPR 2017 and Data Protection Act 2018.
- The staff member responsible for dealing with such requests will ensure that any disclosure made without the consent of the pupil is done in accordance with the data protection and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998. Relevant, confidential information should only be disclosed to:
  - other members of staff on a need to know basis;
  - relevant Parents/Guardians;

- other authorities if it is necessary in the public interest, e.g. prevention of crime;
- other authorities, such as the LEA and Academy's to which a pupil may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other Academy's. DfES/0268/2002 provides further information).

9. Fair Obtaining/Processing

Individuals whose information is collected by the Academy must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of a pupils personal information should take place unless reasonable steps have been taken to make that individual aware of that processing. Pupils must also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information. The pupils and other data subjects will also be informed of the purposes of the processing as well as the legal basis for processing.

Information will also be provided as to how long the information will be kept for, the rights that the pupils can exercise with regards to their data and information to enable pupils to lodge a complaint with the Information Commissioners Office if their rights are not met under the GDPR and DPA 2018.

10. Data Uses and Purposes

All processing of personal data must be for a purpose that is necessary to enable the Academy to perform its duties and services. Personal information should only be processed in line with those notified purposes.

All personal data should be regarded as confidential and its security protected accordingly. This also applies when Academy information is being processed at members of staff's homes. Information held by the Academy must not be used for unauthorised non-Academy purposes. If you become aware of any potential data breach, please refer to section 9 below, and follow the designated procedures accordingly.

Personal Information should only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established, e.g. where the information is required by the police for the prevention and detection of crime, or a relevant Information Sharing Agreement is in place.

Purposes will include the following:

- Providing education and pastoral care
- Providing activities for pupils including Academy trips and after Academy clubs and activities
- Safeguarding and promoting the welfare of children

- Providing references for pupils and staff
- Providing human resources function for staff
- Ancillary purposes to education including completing contractual obligations
- Fundraising.

11. Data Incident Reporting / Data Breach

Staff members must notify the DPO of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. Any reported data incident will be investigated appropriately and actions taken as necessary.

If a member of the public reports a potential incident, they can do this by contacting the Data Protection Officer (Nigel Frost) directly by phone on 0115 917 7202 or by e-mail on DPO@foxwood.notts.sch.uk

Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff members will follow the Academy's Data Breach guidance manual with associated templates and procedures and the Information Commissioner's Office guidance.

12. Data Quality and Retention

Information processed should not be excessive or irrelevant to the notified purposes.

Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the Academy's Retention and Disposal Schedule and contained in the Academys record management policy.

Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

13. Records of processing activities

In order to be able to properly and effectively comply with our obligations under the GDPR and the DPA2018, the Academy needs to fully understand what information it holds and where this information is kept. We also need to consider how we keep this information up-to-date and how we know when to dispose of it. The Academy shall maintain a record of processing which include the following information:

- The name of the Academy and the details of the Data Protection Officer
- The purposes of processing as outlined above in this policy document
- Which condition is relied on and in particular, how the processing satisfies Article 5 and 6
- Set out the ownership, governance and maintenance of Information Assets
- Set out retention and disposal schedule for Information

- Sets out whether the personal data is retained and erased in accordance with the policy and if it is not the reason for not following the policy
- Map the flow of data in and out of the teams within the Academy.

14. Data Security

The Academy must take all appropriate technical and organisational measures to safeguard against unauthorised or unlawful processing of personal information and against accidental loss, damage or destruction of personal information.

All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully. To ensure that an appropriate level of security is afforded to all information the Academy's Information Security Policy will be adhered to at all times.

Everyone managing and handling personal information will be appropriately trained to do so and this will include appropriate refresher training every two years.

All members of staff have a duty to follow this Policy and associated procedures and to co-operate with the Academy to ensure that the aim of this Policy is achieved.

All members of staff must be wary of possible threats the security of personal data, (e.g. computer screens being visible to members of the public who visit the site, etc.) and proactively take steps to mitigate the threats.

Disciplinary action may be taken against any member of staff who fails to comply with or commits a breach of this Policy.

It is the duty of individual members of staff to ensure that personal information held by them is dealt with in accordance with the Act.

Suitable measures should be taken to ensure that any processing of personal data carried out by a third party on behalf of the Academy complies with the Principles of the Act and this Policy. Similarly, when the Academy is processing personal information on behalf of a third party it will need to demonstrate that the information is subject to the same standard of care.

The Data Protection Policy should be read in conjunction with the following:

- Data Breach Guidance
- Freedom of Information Policy
- Records Management Policy
- Acceptable Use policy
- Email policy
- Safeguarding Policy and Guidance.

This page is intentionally blank

DAISI

Data Analysis & Insight for School Improvement

Nottingham City Council