OAKFIELD ACADEMY

BELIEVE AND ACHIEVE

Data Protection Policy

Written/ Reviewed by:	**Business Manager/ Data Manager**
Approved by:	**Data Link Governor/Finance Committee**
Ratified on:	**24th April 2018 by Full Governing Body**
Next review due:	**April 2020** or when new recommendations are made

Data Processing Officer: Ian Gover: Somerset County Council

Academy Data Processing Lead: Sarah Wells Business Manager, Christine Peacock Data Manager

Introduction

The Academy needs to keep information about our pupils, staff and other users to allow us to follow our legal and statutory duties and to provide other services.

The academy will comply with the data protection principles which are set out in the General Data Protection Regulation[i] and other laws.

The Data Controller and the Designated Data Controllers

The Academy, as a body, is the Data Controller.

The Academy has identified its designated Data Protection Officer (DPO) who will deal with matters detailed in appendix A.

Other day to day matters will be dealt with by The Data Protection Leads, The Headteacher and Deputy Headteachers.

Responsibilities of the Academy

The academy is committed to protecting and respecting the confidentiality of sensitive information relating to staff, pupils, parents and governors. This implies that:

a) all systems that involve personal data or confidential information will be examined to see that they meet the General Data Protection Regulations;
b) the academy will inform all users about their rights regarding data protection;
c) the academy will provide training to ensure that staff know their responsibilities;
d) the academy will monitor its data protection and information security processes on a regular basis, changing practices if necessary.

Responsibilities of Staff

All staff are responsible for checking that any information that they provide to the Academy is accurate and up to date.

All staff are also responsible for ensuring that any personal data they use in the process of completing their role:

a) is not in the view of others when being used;
b) is kept securely in a locked filing cabinet or drawer when not being used;
c) be password protected both on a local hard drive and on a network drive that is regularly backed up;
d) if kept on a laptop, USB memory sticks or other removable storage media, is password protected and encrypted. The device must be kept in a locked filing cabinet, drawer, or safe when not in use. The data held on these devices must be backed up regularly;
e) is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure or transgression of the above statements will usually be a disciplinary matter.

Responsibilities of Parents/Guardians

The academy will inform the Parents/Guardians of the importance of and how to make any changes or deletions to personal data. This includes an annual data collection sheet with the return of this document being recorded.

Other permissions will also be sought regarding matters of non-statutory use of personal data such as the use of images and use of names in publicity materials on induction, annually or when required. The returns to these permissions will be recorded and exemptions communicated to staff.

Rights to Access Information

All people having personal data stored by the academy have the rights to:

a) obtain from the academy confirmation as to whether personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
   (i) the purposes of the processing;
   (ii) the categories of personal data concerned;
   (iii) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
   (iv) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
   (v) the existence of the right to request from the academy rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
   (vi) the right to lodge a complaint with a supervisory authority;
   (vii) where the personal data are not collected from the data subject, any available information as to their source;
   (viii) the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

b) know where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards relating to the transfer.

c) have a copy of the personal data undergoing processing. For any further copies requested by the data subject, the academy may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

d) obtain a copy referred to in paragraph c) shall not adversely affect the rights and freedoms of others.

The Academy will place on its website Privacy Notices regarding the personal data held and the reasons for which it is processed.

All staff, parents and other users have a right to ask to view personal data being kept about them or their child called a Subject Access Request. Any person who wishes to exercise this right should make a request in writing and submit it to the Headteacher. The process for dealing with these requests is outlined in Appendix B.

The Academy aims to comply with requests for access to personal information as quickly as possible and in compliance with advice from the Information Commissioner's Office and other professional agencies. There may be an administration charge which will be stated once the enquiry is made.

The process for dealing with Freedom of Information requests is given in Appendix C.

Data Breaches

If there is a Data Breach the academy will inform the DPO who will then advise on any actions.

Any Data Breaches will be recorded, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

If there is a risk to the individual, the academy will communicate the breach to the data subjects.

In the case of a personal data breach where there is a high risk to the rights and freedoms of the data subject, the DPO shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority.

Reporting policy incidents

Any member of staff, parent or other individual who considers that the Policy has not been followed in respect of personal data about himself or herself or their child should raise the matter with the Headteacher, in the first instance. Alternatively, they could contact the DPO directly.

Monitoring and Evaluation

This policy will be monitored and reviewed in line with the academy's policy review procedure.

Appendix A – Role of Data Protection Officer

According to Article 37(5), the DPO, who can be a staff member or contractor, shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39. These are:

- to inform and advise the controller or the processor and the employees who are processing personal data of their obligations pursuant to this Regulation;
- to monitor compliance with this Regulation, including the assignment of responsibilities, awareness- raising and training of staff involved in the processing operations, and the related audits;
- to provide advice where requested about the data protection impact assessment and monitor its performance pursuant to Article 35;
- to cooperate with the supervisory authority (the ICO in the UK);
- to act as the contact point for the supervisory authority on issues related to the processing of personal data.

Appendix B – Process for dealing with Subject Access Request or request for change or deletion of data

On receiving a Subject Access Request or request for change or deletion of data the academy will:

- inform the Data Protection Lead in the academy (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary;
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- make contact with the DPO if clarity on the request is needed or procedure is needed;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than 30 days, which can be extended by a further 2 months where the request is complex or where there are numerous requests.

Appendix C – Process for dealing with Freedom of Information Requests

On receiving a Freedom of Information Request, which must be made in writing, the academy will:

- inform the Data Protection Lead in the academy (and the Headteacher if necessary);
- record the details of the request, updating this record where necessary;
- reply to the requestor informing receipt of the request asking for clarity if there is confusion about which data is required;
- decide that if the material is already published or falls within an exemption;
- contact the DPO if clarity on the request is needed or procedure is needed;
- if data is not going to be published inform the requestor why this is not being released;
- identify the people responsible for gathering the necessary data;
- gather the data indicating a deadline;
- examine the data for redactions making sure there is no 'bleeding' of data;
- ask the requestor for an address and time for delivery.

The whole process should take no longer than 20 working days.

[i] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679