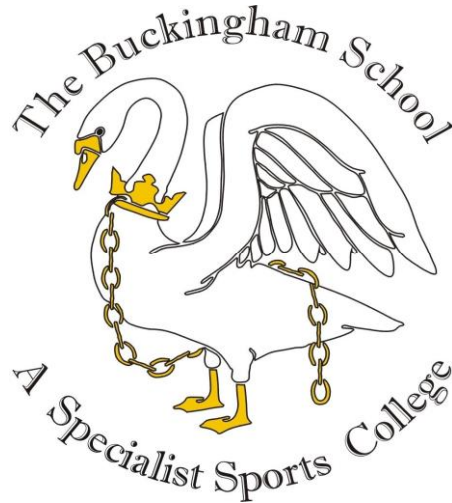


**DATA PROTECTION POLICY  
FOR  
THE BUCKINGHAM SCHOOL  
A SPECIALIST SPORTS COLLEGE**



<b>NAMED PERSON:</b>	<b>BUSINESS MANAGER</b>
<b>ATTACHED COMMITTEE:</b>	<b>FPH&amp;S</b>
<b>ADOPTED:</b>	<b>SEPTEMBER 2012</b>
<b>REVIEW DATE:</b>	<b>SEPTEMBER 2017</b>
<b>REVIEW CYCLE:</b>	<b>1 YEAR</b>
<b>NEXT REVIEW DATE:</b>	<b>SEPTEMBER 2018</b>

# **The Buckingham School Data Protection Policy and Procedures**

## **Introduction**

Our school gathers and uses personal information about staff, pupils, parents and other individuals who come into contact with the school to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations. The detail of this can be found in the school privacy notice on the school website.

## **The Data Protection Officer (DPO)**

The school is required to have a nominated Data Protection Officer. The DPO is tasked with monitoring compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training and audits. The DPO acts as a contact point for the Information Commissioners Office (ICO). They co-operate with the ICO, including during prior consultations under Article 36, and will consult on any other matter.

## **What is Personal Information?**

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

## **Duty on Schools**

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Privacy Notice (see appendix 1 for model) to all pupils/parents, which summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

## **Purpose**

This policy and set of procedures are intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation 2018 (GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files, on tape or disk, or otherwise electronically.

## **GDPA Principles**

The GDPR establishes six enforceable principles that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Personal data shall be 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;
5. Personal data shall be 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 insofar 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 by the GDPR in order to safeguard the rights and freedoms of individuals
6. Personal data shall be processed in a manner that ensure 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.

#### Policy

Our school is committed to maintaining the above principles at all times. Therefore we will:

- Register, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use.
- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely.
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Share information with others only when it is legally appropriate to do so.
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests.
- Issue a Privacy Notice which summarises the information held by us
- Ensure our staff are aware of and understand our policies and procedures.

#### **Rights of access to information**

Pupils, parents and guardians have two distinct rights of access to information held by schools about pupils as set out below.

In addition, the school may hold some information about parents and guardians, and the right of access to this is covered by number one below only:

1. Under the GDPR any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

## **Procedures for responding to Subject Access Requests for access to a person's information made under the GDPR**

### **Actioning a Subject Access Request**

1. Requests for information must be made in writing; which includes email ([DPO@buckinghamschool.org](mailto:DPO@buckinghamschool.org)), and be addressed to the **Data Protection Officer**. If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any information, and when requesting data on a pupil, checks will also be carried out regarding proof of relationship to the child. Evidence of identity will be established by requesting production of a copy of:
  - passport
  - driving licence
  - utility bills with the current address
  - Birth / Marriage certificate
  - P45/P60
  - Credit Card or Mortgage Statement *This list is not exhaustive.*
3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Data Protection Officer should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent, an individual with parental responsibility or guardian shall make the decision on behalf of the child.
4. The school will provide a copy of the information free of charge. However, the school will charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
5. The response time for subject access requests, once officially received, is within one month of receipt of the request. However, this will be extended by up to a further two months where the requests are complex or numerous. The school will inform you within a month of receipt should this be the case and explain why the extension is necessary.
6. The GDPR allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure.**
7. Third party information is that which has been provided by another person. Before disclosing third party information consent will normally be obtained from them. (*There is still a need to adhere to the one month statutory timescale.*)
8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another will not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.
9. If there are concerns over the disclosure of information, then additional advice will be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided will be retained in order to establish, if a complaint is made, what was redacted and why.
11. Information disclosed should be clear, thus any codes or technical terms will be clarified and explained. If information contained within the disclosure is difficult to read or illegible, it will be retyped.
12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant will be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail will be used.

### **Complaints**

Complaints will be dealt with in accordance with the school's complaints procedure, a copy of which can be obtained from the school office.

Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator) [www.ico.gov.uk](http://www.ico.gov.uk) or telephone 0303 123 1113.

### **STAFF ID CARDS**

Staff will be accessing the school site using their own **registered identity card**. These cards will allow staff to access the site at all hours, and ensure safe guarding and GDPR compliance. If your card is misplaced/lost or stolen it must be reported immediately. Staff must wear lanyard ID badges at all times on site and will be charged for loss of cards. On leaving school employment, cards must be returned.

### **Review**

This policy and set of procedures will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The review will be undertaken by the Headteacher, or nominated representative.

### **Contacts**

If you have any enquires in relation to this policy and procedures, please contact the Data Protection Officer, [DPO@buckinghamschool.org](mailto:DPO@buckinghamschool.org) who will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office, [www.ico.gov.uk](http://www.ico.gov.uk) or telephone 0303 123 1113

**THE BUCKINGHAM SCHOOL – A SPECIALIST SPORTS  
COLLEGE**



**DATA PROTECTION**

Adopted:	September 2012
Review Cycle:	1 Year
Review Date:	September 2017
Next Review Date:	September 2018

**Mr Matthew Watkins**

Chairman of  
Governors

Signed: 

Date: September 2017