THE BOURNE ACADEMY

DATA PROTECTION POLICY

VISION

Our central belief is that everyone is a learner and everyone is a teacher

PURPOSE

At The Bourne Academy we develop literate, numerate global citizens who ASPIRE:
Ambitious, **S**elf-confident, **P**hysically Literate, **I**ndependent Learners, **R**esilient, **E**motionally Literate

The General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

POLICY OBJECTIVES

The Academy, as the Data Controller, will comply with its obligations under the GDPR and DPA. The Academy is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the Academy and all staff comply with the legislation.

SCOPE OF THE POLICY

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information[1]. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The Academy collects a large amount of personal data every year including: student records, staff records, parent/carer contact details, examination marks, references, as well as the many different types of research data used by the Academy. In addition, it may be required by law to

[1] GDPR Article 4 Definitions

collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

THE PRINCIPLES

The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**);
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 (**purpose limitation**);
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**);
4. Personal data shall be accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**);
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**);
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information is processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

The Governing Body shall be responsible for, and will be able to demonstrate compliance with, these principles.

TRANSFER LIMITATION

In addition, personal data shall not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data as determined by the European Commission or where the organisation receiving the data has provided adequate safeguards[2].

This means that individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer. It may also be possible to transfer data where the data subject has provided explicit consent or for other limited reasons. Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

LAWFUL BASIS FOR PROCESSING PERSONAL INFORMATION

The purposes for the processing of personal data, and the most appropriate lawful basis for processing the data, must be selected for the data can be processed:

[2] These may be provided by a legally binding agreement between public authorities or bodies, standard data protection clauses provided by the ICO or certification under an approved mechanism.

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Academy;
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- Processing is necessary for compliance with a legal obligation to which the data controller is subject;
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[3]; and
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, the consent from be kept separate from those other matters.

  Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first consented.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the Academy's relevant privacy notices.

SENSITIVE PERSONAL INFORMATION

When sensitive personal data (know as 'special categories of personal data') is being processed then an additional special conditions for processing is identified[4].

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so has been identified
- One of the special conditions for processing sensitive personal information applies:
  (a) the individual ('data subject') has given explicit consent;
  (b) the processing is necessary for employment law purposes;
  (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
  (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim;

[3] The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

[4] GDPR, Article 9

(e) the processing relates to personal data which is manifestly made public by the data subject;
(f) the processing is necessary for the establishment, exercise or defence of legal claims;
(g) the processing is necessary for reasons of substantial public interest;
(h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services; and
(i) the processing is necessary for reasons of public interest in the area of public health.

The Academy's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the Academy can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the Academy can demonstrate compliance with the GDPR.

AUTOMATED DECISION MAKING

The Academy will notify the data subject as soon as reasonable possible when decisions have been made in the process of personal data processing using solely automated decision making, along with the significance and envisaged consequences of the processing. The data subject may object to such decision making and /or request the Academy to reconsider.

DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

All data controllers are required to implement 'Privacy by Design' when processing personal data. This means that the Academy's processes must incorporate appropriate technical and organisational measures effectively to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

The Academy will refer to the Department of Education's DPIA template when carrying out such assessments and consult with the DPO for support and guidance prior to DPO sign off on completion.

DOCUMENTATION AND RECORDS

Written records of processing activities must be kept and recorded, including:

- the name(s) and details of individuals or roles that carry out the processing;
- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;

- retention schedules; and
- a description of technical and organisational security measures.

As part of the Academy's record of processing activities the DPO will document, or link to documentation on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal information;
- DPIAs; and
- Records of data breaches.

Records of processing of sensitive information are kept on:

- The relevant purposes for which the processing takes place, including why it is necessary for that purpose;
- The lawful basis for our processing; and
- Whether the personal information is retained or erased in accordance with the Retention Schedule and, if not, the reasons for not following the policy.

The Academy should conduct regular reviews of the personal information it processes and update its documentation accordingly. This may include:

- Carrying out information audits to find out what personal information is held;
- Talking to staff about their processing activities; and
- Reviewing policies, procedures, contracts and agreements to address retention, security and data sharing.

PRIVACY NOTICES

The Academy will issue privacy notices as required, informing data subjects about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

When information is collected directly from data subjects, including for HR or employment purposes, the data subject shall be given all the information required by the GDPR including the identity of the data controller and the DPO, how and why the Academy will use, process, disclose, protect and retain that personal data through a privacy notice (which must be presented when the data subject first provides the data).

When information is collected indirectly (for example from a third party or publicly available source) the data subject must be provided with all the information required by the GDPR as soon as possible after collecting or receiving the data. The Academy must also check that the data was collected by the third party in accordance with the GDPR and on a basis which is consistent with the proposed processing of the personal data.

The Academy will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

PURPOSE LIMITATION

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

Personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained unless the data subject has been informed of the new purposes and they have consented where necessary.

DATA MINIMISATION

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The Academy maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time.

INDIVIDUAL RIGHTS

Data subjects have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed;
- To request access to any personal data The Academy holds about them, via a Subject Access request;
- To have data corrected if it is inaccurate or incomplete;
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten');
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the Academy no longer need the personal information, but you require the data to establish, exercise or defend a legal claim;
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the Academy are verifying whether it is accurate), or where you have objected to the processing (and the Academy are considering whether the Academy's legitimate grounds override your interests);
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format;
- To withdraw consent to processing at any time (if applicable);
- To object to decisions based solely on automated processing;
- To be notified of a data breach which is likely to result in high risk to their rights and obligations; and
- To make a complaint to the ICO or a Court.

INDIVIDUAL RESPONSIBILITIES

During their employment, staff may have access to the personal information of other members of staff, students, parents/carers, suppliers or the public. The Academy expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;

- only allow individuals who are not Academy staff to access personal information if you have specific authority to do so;
- keep personal information secure;
- not remove personal information, or devices containing personal information from the Academy's premises unless appropriate security measures are in place; and
- not store personal information on local drives or on personal devices that are used for work purposes.

INFORMATION SECURITY

The Academy will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their Academy's acceptable usage policy.

The Academy will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Academy has implemented and maintains in accordance with the GDPR and DPA.

Where the Academy uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the Academy;

- those processing data are subject to the duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the Academy and under a written contract;
- the organisation will assist the Academy in providing subject access and allowing individuals to exercise their rights in relation to data protection;
- the organisation will delete or return all personal information to the Academy as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide the Academy with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Academy immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

STORAGE AND RETENTION OF PERSONAL INFORMATION

Personal data will be kept securely in accordance with the Academy's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Data is retained in line with the Academy's retention policy.

DATA BREACHES

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored;
- Unauthorised access to or use of personal information either by a member of staff or third party;
- Loss of data resulting from an equipment or systems (including hardware or software) failure;
- Human error, such as accidental deletion or alteration of data;
- Unforeseen circumstances, such as a fire or flood;
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- Blagging offences where information is obtained by deceiving the organisation which holds it.

The Academy must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The Academy must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager and DPO immediately when a data breach is discovered and make all reasonable efforts to recover the information, following the Academy's agreed breach reporting process.

TRAINING

The Academy will ensure that staff are adequately trained regarding their data protection responsibilities.

CONSEQUENCES OF A FAILURE TO COMPLY

The Academy takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Academy and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the Academy's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the Academy's DPO.

MONITORING, EVALUATION AND REVIEW

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Governing Body will review this policy at least every three years and assess its implications and effectiveness. The policy will be promoted and implemented throughout the Academy.

Policy written by the Principal in consultation with staff in May 2018

Signed off by The Chair of Governors on behalf of the Governing Body on

Next review date – May 2021