



## DATA PROTECTION POLICY

<b>Policy Number</b>	0029	<b>Policy Author</b>	M Sherman
<b>Date of Issue/Reviewed</b>	July 2023	<b>Policy Ownership</b>	Finance & Operations
<b>Agreed by Governors</b>	July 2017	<b>Date of Next Review</b>	July 2024

## Contents

<b>Section</b>	<b>Description</b>	<b>Page</b>
<b>PART A</b>	Introduction	3
	Application	3
	Revision	3
	Distribution	3
	Duties and Responsibilities	3
	Interpretation	3
<b>PART B</b>	<b>Policy Statement</b>	
	Compliance	4
	Data Gathering	4
	Processing	4
	Data Storage	5
	Data Checking	5
	Data Disclosures	5/6
	Confidentiality	6
	Ownership of Data	6
	Training	6
<b>Appendix 1</b>	Data Retention Guidelines	7

## **PART A**

### **1. Application**

- 1.1 This policy applies to all personal data held at The Basildon Academies. It encompasses paper records, data held on computer and associated equipment of whatever type and at whatever location, used by or on behalf of The Academies.
- 1.2 The obligations outlined in this policy apply to all those who have access to personal data, whether they are employees, governors, employees of associated organisations or temporary staff. It includes those who work from home, who must follow the same procedures as they would in an office environment.
- 1.3 Any individual who knowingly or recklessly processes or divulges data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy.

### **2. Revision**

- 2.1 This document will be reviewed by the Senior Leadership Team annually and any amendments presented to the Governing Body for approval.

### **3. Distribution**

- 3.1 This policy can be found on The Basildon Academies website.

### **4. Duties and responsibilities**

- 4.1 It is the responsibility of the Governing Body to establish, maintain and monitor relevant policies, codes and procedures. Staff of the Academy should familiarise themselves with the contents of this code and should act in accordance with the principles set out in it. Specific reference will be made to this policy in the induction process for all staff of the Academies.
- 4.2 Line Managers are responsible for the discipline of the employees whom they manage and for ensuring that employees are aware of the Academy policies.
- 4.3 All staff are required to comply with this policy, and to participate in the procedure where this is required of them. Not doing so could result in disciplinary action.

### **5. Interpretation**

- 5.1 Any question as to the interpretation or application of this procedure shall be determined by the Governing Body Staffing Committee.

## **PART B**

### **POLICY STATEMENT**

#### **1. The Basildon Academies will comply with:**

1.1 The terms of General Data Protection Regulation (GDPR) and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

1.2 The eight enforceable principles of good practice contained in the General Data Protection Regulation (GDPR). These state that personal data must be: -

- Fairly and lawfully processed;
- Obtained only for one or more specified and lawful purposes;
- Adequate, relevant & not excessive in relation to the purpose for which it is processed;
- Accurate and kept up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the data subject's rights;
- Secure;
- Not transferred to a country outside the EEC unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

1.3 The guidance displayed on the Information Commissioner's website (<http://ico.org.uk>) and published in "the Guide to Data Protection" published by the Information Commissioner's office and is available at the following web address: <https://ico.org.uk/for-organisations/guide-to-data-protection/>

#### **2. Data Gathering**

2.1 Only relevant personal data may be collected and the person from whom it is collected will be informed why the data is being collected, of the data's intended use and any possible disclosures of the information that may be made.

#### **3. Processing**

3.1 All processing of personal data will comply with the Data Protection Principles as defined in General Data Protection Regulation (GDPR). In the situation where data is processed by a third party, the third party will be required to act in a manner that ensures compliance with General Data Protection Regulation (GDPR).

3.2 Data will only be processed for the purpose for which it was collected and will not be used for incompatible purposes without the consent of the data subject.

#### **4. Data Storage**

- 4.1 The Basildon Academies will hold the minimum amount of personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed. Details relating to relevant deadlines are summarised in Appendix 1.
- 4.2 The Basildon Academies will store personal data in a secure and safe manner.
- 4.3 Electronic data will be protected by standard password and firewall systems operated by The Basildon Academies.
- 4.4 Computer workstations in administrative areas will be positioned so that they are not visible to casual observers.
- 4.5 Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.
- 4.6 Particular attention will be paid to the need for security of sensitive personal data.

#### **5. Data Checking**

- 5.1 The Basildon Academies will issue regular reminders to staff and parents/carers to ensure that personal data held is up-to-date and accurate.
- 5.2 Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

#### **6. Data Disclosures**

- 6.1 Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.
- 6.2 When requests to disclose personal data are received by telephone it is the responsibility of the member of staff taking the call to ensure the caller is entitled to receive the data and that they are who they say they are. It is advisable to call them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.
- 6.3 If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.
- 6.4 Requests from parents/carers or students for printed lists of the names of students in particular groups, which are frequently sought at Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list. (Note: A suggestion that the child makes a list of names when all the students are present in class will resolve the problem.)

- 6.5 Personal data will not be used in newsletters, websites or other media without the consent of the data subject.
- 6.6 Routine consent issues will be incorporated into The Academy's student data collection sheets, to avoid the need for frequent, similar requests for consent being made by The Basildon Academies.
- 6.7 Personal data will only be disclosed to Police Officers if they are able to supply a relevant document which notifies of a specific, legitimate need to have access to specific personal data.
- 6.8 A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

## **7. Confidentiality and Security**

- 7.1 Personal data is confidential and confidentiality must be preserved in compliance with the Data Protection Principles as defined in General Data Protection Regulation (GDPR) list.
- 7.2 Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.
- 7.3 Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the school's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.

## **8. Ownership of Data**

- 8.1 The Basildon Academies are responsible for the personal data that it holds. This responsibility extends to any data that is processed by a third party.

## **9. Training**

- 9.1 All staff working with personal data must understand the importance of adhering to the General Data Protection Regulation (GDPR) Principles. Training will be provided to staff annually and as part of the Induction process for new starters.

## Data Protection Summary

### What must I do?

1. **MUST:** All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals
2. **MUST:** Where personal data is used, we must make sure that the data subjects have access to a complete and current **Privacy Notice**.
3. **MUST:** We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which involves the use of personal data
4. **MUST:** We must process only the **minimum** amount of personal data necessary to deliver services.
5. **MUST:** All employees who record **opinions** or intentions about students, parents/carers or staff must do so carefully and professionally
6. **MUST:** We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. **MUST:** We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition
8. **MUST:** Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services.
9. **MUST:** Consent will **expire** at the end of each 'Key Stage' period unless it is reconfirmed.
10. **MUST:** We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
11. **MUST:** If we receive a **request** from a member of the public or colleagues asking to access their personal data, we must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the [Education \(Pupil Information\) \(England\) Regulations 2005](#)
12. **MUST:** If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we must fully consider Data Protection law before disclosing it
13. **MUST:** When someone contacts us requesting we change the way we are processing their personal data, we must consider their **rights** under Data Protection law.
14. **MUST NOT:** You must not access personal data which you have **no right to view**
15. **MUST:** You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so
16. **MUST:** You must **share** personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer (DPO) or Senior Information Risk Owner (SIRO)
17. **MUST:** Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice.

18. **MUST:** All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely. This training must be regularly refreshed to ensure knowledge remains current.
19. **MUST:** When using '**data matching**' techniques, this must only be done for specific purposes in line with formal codes of practice, informing students, parents/carers or staff of the details, their legal rights and getting their consent where appropriate.
20. **MUST:** We must pay an annual [Data Protection Fee](#)
21. **MUST:** Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we must follow the relevant procedure
22. **MUST NOT:** You must not **share** any personal data held by us with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or Data Protection Officer
23. **MUST:** We must identify **Special Categories** of personal data and make sure it is handled with appropriate security and only accessible to authorised persons
24. **MUST:** When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method

## Why must I do it?

1. To comply with legislation
2. To comply with Data Protection legislation which requires us to make the data subject aware of how we will handle their personal data
3. To ensure that the rights of the Data Subject are protected in any proposed new activity or change to an existing one
4. The law states that we must only process the minimum amount of information needed to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
5. To maintain professional standards and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
6. To comply with a principle of Data Protection law
7. To comply with Data Protection law. Where processing does not rely on a legal condition other than consent
8. When using personal data for marketing and promoting services it is unlikely that any lawful condition other than consent would apply.
9. Consent can only be valid for a reasonable period of time.
10. To comply with a principle of Data Protection law.
11. To comply with the right to access personal data
12. To comply with a principle of Data Protection law
13. To comply with the rights of the Data Subject under Data Protection law



14. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
15. Personal data must be protected by effective security controls to ensure that only those with approved business need to access the data can do so
16. To comply with the legal requirements to keep personal secure but also to ensure that where there are legal grounds to share information in a managed way that this is done correctly.
17. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain circumstances recordings may be accessed e.g. to investigate alleged criminal activity or breaches of Organisation policy etc.
18. To comply with a principle in Data Protection law, regulatory guidance and the Data Protection Officer governance requirements.
19. To comply with the Data Subject's rights
20. This is a regulatory requirement
21. Where personal data is used for research purposes, the processing of the data can be legitimised by provisions within Data Protection law
22. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here. Personal data transferred overseas (including hosted solutions) must be securely handled under the same or substantially similar provisions that exist under the Data Protection Act.
23. To comply with Article 9 of GDPR
24. To comply with Article 9 of GDPR and comply with a principle of Data Protection law requiring that personal data is processed with appropriate security measures

## **How must I do it?**

1. By following the points in this policy
2. By approving and reviewing a compliant privacy notice in line with the Privacy Notice Procedure and making it available to the data subjects
3. By completing and approving a Privacy Impact Assessment, or Data Protection Impact Assessment where the processing is 'high risk' to the rights of the data subjects.
4. By ensuring that the means we use to gather personal data (such as forms etc.) only ask for the information that is required in order to deliver the service.
5. By considering that anything committed to record about an individual may be accessible by that individual in the future or challenged over its accuracy.
6. For example, there should be at least an annual check of the currency of data held about students, parents/carers or staff and whenever contact is re-established with a service user, you should check that the information you hold about them is still correct.
7. By following the points in the Consent Procedure

8. By following the points in the Consent Procedure
9. By following the points in the Consent Procedure. Parents/ Guardians of pupils in the last year of a key stage should expect a communication to ask them to refresh their consents. If they do not respond ahead of a deadline date then consent should be assumed to be no longer valid.
10. By following the points in the Records Management Policy. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the law allows us to keep indefinitely personal data processed only for historical, statistical or research purposes. The Retention Schedule will give guidance in these areas.
11. By following the points in the Statutory Requests for Information Policy. We must be aware that data subjects can ask others to make a request on their behalf. There must be evidence of consent provided by the Data Subject to support this.
12. By following the points in the Statutory Requests for Information Policy. Such requests would typically be managed under the Freedom of Information Act (if from a member of the public) or under Data Protection or Justice law if for a criminal investigation, however the decision whether or not to disclose someone's personal data to a third party must satisfy the requirements of Data Protection law
13. By reviewing the impact of any requested change on any statutory duty being fulfilled by the Organisation.
14. By being aware through training and guidance from your manager on what information is appropriate for you to access to do your job. Systems and other data storage must be designed to protect access to personal data. You must inform your manager if you have access to data which you suspect you are not entitled to view.
15. By ensuring appropriate security controls are in place and rules to support those controls are followed. The following should be in place:
  - technical methods, such as encryption, password protection of systems, restricting access to network folders;
  - physical measures, such as locking cabinets, keeping equipment like laptops out of sight, ensuring buildings are physically secure; and
  - organisational measures, such as:
    - Providing appropriate induction and training so that staff know what is expected of them
    - Taking reasonable steps to ensure the reliability of staff that access personal data, for example, by the use of Disclosure and Barring Service (DBS) checks.
    - Making sure that passwords are kept secure, forced to be changed after an agreed period and are never shared
16. Consult your manager, any procedure guidance or any library of sharing agreements managed by the Organisation. Consult the Data Protection Officer or SIRO in one-off cases of sharing.

17. By ensuring that employees and members of the public are fully aware of what personal data is being recorded about them and why, and in what circumstances that data may be used. Operation of overt surveillance equipment such as CCTV must always be done in line with relevant codes of practice captured in the Surveillance Management Procedure. Any covert surveillance must be done in line with the provisions in the Investigatory Powers Act (2016)
18. By completing compulsory training courses relevant to your role. Records will be kept of induction training and annual refresher training. Training content for each role will be determined by feedback on current training methods and the outcome of investigating data breaches. This will be reviewed frequently.
19. By ensuring an Impact Assessment has been approved for the activity
20. The payment must be made annually to the Information Commissioner's Office (ICO)
21. Follow the guidance in the Data Minimisation Procedure
22. Consult the Data Protection Officer over any proposed sharing outside of the UK. If you are a manager who is proposing a change to or implementing a new system which may involve the hosting of personal data in a nation outside the UK, this must be first assessed by a Privacy Impact Assessment, which must be approved by your SIRO and Data Protection Officer
23. Special Categories of Personal Data are information revealing *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data* for the purpose of uniquely identifying an individual, *data concerning health or data concerning an individual's sex life or sexual orientation*. Where this data is held it should be stored securely and in a way that access is restricted only to those internal staff that have a valid need to access it. It should only be shared externally after verifying that the recipient is entitled to access this data and through secure means.
24. Hard-copy packages must be marked as such by writing on the exterior of the package. Emails should contain the wording in the 'subject' field before the email title. Refer to the Records of Processing Activity document and the register of Data Flows for clear instruction on how you are expected to handle sending the data securely according to the particular activity you are undertaking

### **What if I need to do something against this policy?**

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting the school office.

## APPENDIX 1 - Data Retention Guidelines

The following table illustrates, for guidance purposes, the length of time records need to be kept for legal reasons. This covers the main areas but if you are unsure about a particular record please seek further advice by contacting the Director of Finance and Operations.

Type of Data	Retention Period	Reason
Staff personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References, potential litigation, Legal, financial
Staff application forms/interview notes	6 months from the date of the application	Time limits on litigation
DBS certificate	6 months after the date of the disclosure	Guidelines
Unfounded child protection allegation against staff member	10 years from allegation date	Education Act 2002 guidance
Income Tax and NI returns, including correspondence with tax office	7 years after the end of the financial year to which the records relate	Income Tax [Employment] Regulations 1993
Statutory Sick Pay records and calculations	7 years after the end of the financial year to which the records relate	Statutory Sick Pay [General] Regulations 1982
Wages and salary records	6 years	Taxes Management Act 1970
Accident books; records and reports of injuries and diseases	Staff: 3 years after the date of last entry Students: DOB + 25 years	Social Security (Claims and Payments) Regulations 1979; RIDDOR 1995
Approved Education Visit forms	Date of visit + 10 years	Health and Safety of Pupils on Educational Visits (1998)
Pupil Statement information	DOB + 30 years	SEN and Disability Act 2001
Student files, Child protection files	DOB + 25 years	Education Act 2002 s175
Meeting notes and other records created by Exec. Management; visitor log	6 Years	Academy Operating rule