Schools Data Protection Policy
Badgerbrook Primary School, Whetstone

1. Introduction

The purpose of this policy is to ensure that Badgerbrook Primary School and individuals working for, or on its behalf, are aware of their obligations under, and comply with, UK Data Protection Law.

Badgerbrook Primary School collects and processes different types of information about, the pupils that study at the school, their parents and people who it deals and communicates with in order to provide an education for its students.

It is the school's obligation, as the Data Controller, to ensure compliance with UK Data Protection Law.

The following policy outlines the school's responsibilities and processes surrounding the personal data which is processed by the school and its employees.

2. Scope

This policy applies to:

- All forms of information and data owned, administered, stored, archived or controlled by the school, including electronic and hard copy formats,
- Information and data in test, training and live environments, however it is hosted.
- All employees of the school including temporary and contract staff, volunteers, governors and third-parties accessing or using the school's information, data and/or network; and
- All electronic and communication devices owned, administered, controlled or sanctioned for use by the school.
- All students, parents and members of the public whose personal information is held by the school in order to provide an education

3. Policy Statement

The School has to collect and use personal and/or sensitive information about people in order to operate. This includes information about;

- Parents, Members of the public, students, governors, clients and customers.
- Current, past and prospective employees.
- Suppliers and other third parties.

In addition, the school may have to collect and use information in order to comply with the legal requirements of the Department of Education. This personal information must also be handled in line with the law.

Therefore the School is committed to:

- complying with both law and good practice.
- respecting individuals' rights.
- being open and honest with individuals whose data is collected and held.
- providing training and support for staff who handle personal data, so that they can act confidently and consistently.
- ensure retention & disposal of personal information is adhered to.
- Implement appropriate technical and organisational security measures to safeguard personal information are in place.
- ensure personal information is not transferred abroad without suitable safeguards or adequate protection.
- ensure the quality of information used by the School.

To this end the School will only process personal or special category data where an appropriate legal basis can be identified.

The lawful bases for processing are set out in Article 6 of the General Data Protection Regulations (GDPR). At least one of these must apply whenever the School is processing personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

If the School is processing special category data then both an article 6 and article 9 conditions are required. The article 9 conditions are detailed below:

a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law

provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. 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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. processing relates to personal data which are manifestly made public by the data subject;

f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim

pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Further conditions are available within the Data Protection Act 2018. For help and advice in determining the appropriate condition contact the Data Protection Lead at the school.

Where the School is processing personal data it fully endorses and follows the principles of GDPR outlined below.

Personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

b. 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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

d. 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');

e. 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f. 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').

Furthermore the School is responsible for, and must be able to demonstrate compliance with the 6 principles above ('accountability').

4. Data Protection Officer (DPO)

The school shall appoint a Data Protection Officer in line with the requirements of the GDPR.

The School's Data Protection Officer is JA Walker, Solicitor:
Office 7, The Courtyard
Gaulby Lane
Stoughton
Leicestershire
LE2 2FL

Telephone number: 03337729763
info@jawalker.co.uk

The School Business Manager, Mrs C Webb, is the lead person for Data Protection in school.

5. Duties & Responsibilities

The Digital Economy Act 2017 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which the School must be registered

The School will review the Data Protection Register (https://ico.org.uk/esdwebpages/search) annually, prior to renewing its notification to the Information Commissioner.

The responsibility for the fair and lawful processing of personal and/or sensitive personal information at the school rests with the Governors. The Chair of Governors has overall responsibility on behalf of the School as a whole. The day-to-day responsibility of implementation rests with the DPO.

However it is the responsibility of all employees and governors to handle information and data correctly. As an individual representing, working for, or on behalf of, the School it is essential that you understand and abide by the following:

- School policy, procedures and guidance on the collection and use of personal/sensitive information and data;
- Only process personal/sensitive personal information in accordance with the Act;
- Be clear why you are using personal/sensitive information;
- Tell people why their information is being collected, what it will be used for and how it will be managed from collection to destruction through a fair processing notice that meets the requirements of the General Data Protection Regulation;
- Collect only the minimum amount of personal/sensitive data needed, and use it only for the purposes specified or in line with legal requirements;
- Only access the personal/sensitive data that you require to carry out your role and no more;
- Ensure the personal/sensitive information is input correctly and accurately
- Ensure personal/sensitive information is destroyed securely when it is no longer required;
- If you receive a request from an individual for information held by the School about them please refer to the school's DPO;
- Handle all personal information in accordance with the School's security policies and procedures;

- Don’t send personal/sensitive personal information outside of the UK without referring to the DPO;
- Understand and undertake the mandatory training relating to Data Protection and Information Security and annual refresher training.

The School’s Data Protection Officer will:-

- Provide guidance, support and leadership on data protection legislation and regulation across the school or trust working with all teams as required.
- Review the Audit process and outcomes to ensure compliance.
- Advise about changes needed to secure the standard required by the GDPR identified through gap analysis.
- Together with the Data Protection Lead, provide strategic advice on information security matters to ensure compliance with data privacy laws and regulations, international security standards and protection of data against unlawful access, sharing or loss.
- Review, carry out or assess regular risk assessments of the handling of data and maintain & update the risk register.
- Advise about how and when Privacy Impact Assessments should be carried out. Provide support as required.
- Support the process of managing any data security breaches. This may involve coordinating and/or and investigating the breach.
- Advise, support and/or manage all data protection complaints and data security breaches.
- Cooperate with and act as the contact point for the Information Commissioner’s Office or the relevant supervisory authority on issues relating to processing and consult, where appropriate, with regard to any other matter.
- Advise and support drafting, implementation, and maintenance and review of appropriate privacy policies, procedures, and notices of privacy practices.
- Monitor and keep up to date with privacy developments and governance strategies for data management that are relevant in the educational setting.
- Work with relevant IT professionals to ensure that there is compliance with data security measures within the trust or school.
- Support or review retention and data cleansing into systems used to manage personal data in compliance with school or trust obligations.
- Assist in handling data audits by outside agencies.
- Review or support or provide relevant data privacy training for the school community.
- Ensure that governors/trustees, senior management and staff are regularly briefed on relevant developments.
- Maintain a privacy knowledge base of relevant laws, guidance and advice across all jurisdictions as required.
- Provide pragmatic, quality and timely ad hoc advice to all areas of the trust or school to ensure all new initiatives comply with the DPA, GDPR and future legislation as that arises.

- Support, advise or review the Privacy by Design ethos so that it is secured within the school or trust.
- Advise on management of incidents involving loss of personal data.
- Develop, advise, support or review relevant policies and procedures in preparation for GDPR
- Consider arrangements for third parties and obligations to secure agreement to GDPR principles

6. Data Subjects Rights

The GDPR outlines several data subject rights and the School will ensure that the rights of people about whom information is held can be fully exercised. The rights are as follows:

The right to be informed

Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.

The right of access (also known as Subject Access Requests)

Any person whose details are held by the School is entitled to ask for a copy of information held about them (or child for which they are responsible). They are entitled to see if the data held is accurate, and who it is shared with.

Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

This School must provide a copy of the information free of charge. However, a 'reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee must be based on the administrative cost of providing the information.

Information must be provided without delay and at the latest within one month of receipt and in some instances, for education records, 15 school days.

This can be extended by a further two months where requests are complex or numerous. If this is the case, the Council must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the School can:

- charge a reasonable fee taking into account the administrative costs of providing the information;
- or refuse to respond.

Where the School refuses to respond to a request, it must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.
The school must verify the identity of the person making the request, using 'reasonable means'.

If the request is made electronically, the School should provide the information in a commonly used electronic format.

If you receive a subject access request please contact the DPO at the school.

Further guidance is available via the 'Schools Guidance on Subject Access Requests'.

The right to rectification

Individuals have the right to have inaccurate personal data rectified, or completed if it is incomplete.

An individual can make a request for rectification verbally or in writing.

The School has one calendar month to respond to a request.

In certain circumstances you can refuse a request for rectification.

Contact the school DPO should you receive a request of this nature.

The right to erasure

Individuals have a right to have personal data erased.

The right to erasure is also known as 'the right to be forgotten'.

Individuals can make a request for erasure verbally or in writing.

You have one month to respond to a request.

The right is not absolute and only applies in certain circumstances.

Contact the school DPO should you receive a request of this nature.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data.

This is not an absolute right and only applies in certain circumstances.

When processing is restricted, the School is permitted to store the personal data, but not use it.

An individual can make a request for restriction verbally or in writing.

The School have one calendar month to respond to a request.

This right has close links to the right to rectification (Article 16) and the right to object (Article 21).

Contact the school DPO should you receive a request of this nature.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data

Contact the school DPO should you receive a request of this nature.

The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling);
- and processing for purposes of scientific/historical research and statistics.

Objections where the School processes personal data for the performance of a legal task or my organisation's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

The School must stop processing the personal data unless:
it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
or the processing is for the establishment, exercise or defence of legal claims.

The School will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the School processes personal data for direct marketing purposes?

The School must stop processing personal data for direct marketing purposes as soon as it receives an objection. There are no exemptions or grounds to refuse.

The School must deal with an objection to processing for direct marketing at any time and free of charge.

The School will inform individuals of their right to object "at the point of first communication" and in its Fair Processing Notice.

Objections where the School processes personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If the School is conducting research where the processing of personal data is necessary for the performance of a public interest task, it is not required to comply with an objection to the processing.

Contact the school DPO should you receive any requests outlining an objection to processing.

Rights in relation to automated decision making and profiling.

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement);
- and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The GDPR applies to all automated individual decision-making and profiling.

This type of decision-making can only be done where the decision is:

- necessary for the entry into or performance of a contract;
- or authorised by Union or Member state law applicable to the controller;
- or based on the individual's explicit consent.

If the School is conducting this type of decision making it must:

- give individuals information about the processing;
- introduce simple ways for them to request human intervention or challenge a decision;
- carry out regular checks to make sure that your systems are working as intended.

If you wish to process information in this way then contact the school DPO prior to doing so.

7. Fair Processing Notices (Privacy Notice)

Whenever information is collected about individuals they must be made aware of the following at that initial point of collection

- The identity of the data controller, e.g. the School;
- Contact details of the Data Protection Officer;
- The purpose that the information is being collected for;
- Any other purposes that it may be used for;
- What the lawful basis is for processing the data;
- Who the information will or may be shared with;

- If the data is transferred outside of the EU, and if yes, how is it kept secure;
- How long the data will be kept for; and
- How data subjects can exercise their rights.

8. Provision of Data to Children

In relation to the capacity of a child to make a subject access request, guidance provided by the Information Commissioner's Office has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may of course reach sufficient maturity earlier; each child should be judged on a case by case basis.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and receive a response.

Pupils who submit requests to access their educational records should be allowed to do so unless it is obvious that they do not understand what they are asking for.

9. Parents' Rights

An adult with parental responsibility can access the information about their child, as long as the child is not considered to be sufficiently mature. They must be able to prove their parental responsibility and the School is entitled to request relevant documentation to evidence this as well as the identity of the requestor and child. The School has the right to ask the Child if they object to release of information to the Parent if the Child is deemed mature enough to make such a decision.

In addition, parents have their own independent right under The Education (Pupil Information) (England) Regulations 2000 of access to the official education records of their children. Students do not have a right to prevent their parents from obtaining a copy of their school records (as defined in the Education Act).

10. Special category Data

There are additional requirements placed upon the data controller where the holding of "special category data" is concerned. Special category data relates to the following:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Where the School processes any of the above categories of sensitive personal data there should be higher levels of security in place and greater restrictions on sharing and processing this data. Extra care should be given when you process sensitive personal data and more information can be found in the School's Guide to information levels (classification) (Appendix 1) which gives sensitive personal data a level 3 classification. If any guidance is required please contact the School DPO

11. Information Sharing

Where the School regularly shares personal information with partners and other organisations an Information Sharing Agreement should be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection. Any School department which shares personal information externally on a regular basis should contact the school's DPO.

12. Consent

Where the School processes data with consent (for example, to publish photographs of children, to send direct marketing emails about school uniform for sale) it will ensure that the consent is freely given, specific, informed and unambiguous, and the consent is recorded and reviewed regularly

13. Information Society Services

Where the School offers Information Society Services (online services with a commercial element) targeted at children, it will take reasonable steps to seek the consent of the child's parent or guardian if the child is less than 13 years of age

14. Use of personal data in marketing or promotion

Badgerbrook Primary School complies with the Privacy of Electronic Communications Regulations (PECR).

PECR is a law in the UK which makes it unlawful to send direct marketing (or any promotional material with regards to goods and services) by electronic means without the consent of the receiver.

Where the School sends any direct marketing (the promotion of aims and ideals as well as selling goods and services) via electronic communications e.g. email, SMS text, fax or recorded telephone messages, it will only do so if the recipient has given explicit consent to receive them e.g. has ticked a box to 'opt in.'

For further advice please contact the school's DPO.

15. Photographs

Whether or not a photograph comes under the data protection legislation is a matter of interpretation and quality of the photograph. However, the School takes the matter extremely

seriously and seeks to obtain parents' permission for the use of photographs outside the School and, in particular, to record their wishes if they do not want photographs to be taken of their children

16. Responsibility of staff and governors

All staff and governors, whether permanent or temporary, are required to read, understand and accept any policies and procedures that relate to personal data that they may handle in the course of their work.

All have a responsibility for Data Protection and are required to follow this policy.

All have a responsibility to ensure they have completed the mandatory Data Protection and Information Security training.

The Data Protection Policy sits in accordance with the other policies and processes as adopted by the school to ensure compliance with GDPR. These policies should be read in conjunction and contain further guidance in some areas of Data Protection.

Retention and Disposal

The school will create and follow a Data Retention and Disposal Policy. This policy should explain the steps to take to prevent the inappropriate disposal of records and ensure that their final disposal is in accordance with legislation, guidance or good practice.

Further guidance on Data Retention and documenting how long schools need to retain information is available in the **DfE Data protection toolkit for schools**.

Information Security and Acceptable Use Policy

The Schools Information Security and Acceptable Use Policy will give you information on how to comply with Data Protection requirements for the appropriate technical and organisational measures.

17. Data Protection Governance

The following outlines the reporting arrangement around Data Protection within the School:

- Annual Report to the Board of Governors on GDPR compliance
- Quarterly reports on Incidents
- Any reports as required by the Board of Governors

18. Policy Review

A review of this policy will take place at least annually or as required to take account of any new or changed legislation, regulations of business practices.

19. Breaches of this policy and data breaches

Failure to adhere to this policy will place the School at significant risk and may also result in a breach of legislation.

All data breaches and suspected breaches of this policy must be reported via the DPO. Please contact the School's Data Protection lead for more details.

Actions or neglect leading to a breach of this policy, or failure to report a breach will be investigated.

20. Monitoring

All activity and information placed on or sent over School systems should be monitored. Logs created as part of this monitoring can be used to investigate suspected unauthorised use or breach of the Information Security and Acceptable Use Policy. For third party systems these logs must also be created and made available to the School on request.

This Policy was adopted by the Governing Body in November 2021, and will be reviewed and approved annually.

Signed:  Date: 17 November 2021

Chair of Governors