Barnwood Park

DATA PROTECTION POLICY

Date of Policy	June 2022
Date of Next Review	June 2024
Staff Responsible	Business Manager/Headteacher/DPO
School/Governor Policy	Governor – Finance & FGB

Contents:

1. Introduction

In order to operate efficiently Barnwood Park School has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition it may be required by law to collect and use information in order to comply with the requirements of central government.

The School is committed to ensuring personal information is properly managed and that it ensures compliance with the General Data Protection Regulation 2018 [GDPR]. The School will make every effort to meet its obligations under the legislation and will regularly review procedures to ensure that it is doing so.

2. Scope

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff working for or on behalf of the School.

This policy applies to all personal information created or held by the School in whatever format (e.g. paper, electronic, email, microfiche, film) and however it is stored, (for example ICT system/database, shared drive filing structure, email, filing cabinet, shelving and personal filing drawers).

The GDPR does not apply to access to information about deceased individuals.

3. Responsibilities

The Governors have overall responsibility for compliance with the GDPR.

The Headteacher is responsible for ensuring compliance with the GDPR and this policy within the day to day activities of the School.

The Data Protection Officer (DPO) is responsible for ensuring that appropriate training is provided for all staff, as well as conducting audits to ensure compliance and address potential

issues. The DPO will also be the point of contact between the School and the supervisory authority.

All members of staff or contractors who hold or collect personal data are responsible for their own compliance with the GDPR and must ensure that personal information is kept and processed in-line with the GDPR.

4. The Requirements

The GDPR stipulates that anyone processing personal data must comply with seven principles of good practice; these principles are legally enforceable. The principles require that personal information:

1. **Lawfulness, fairness and transparency**
   Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. **Purpose limitation**
   Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. **Data minimisation**
   Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. **Accuracy**
   Personal data shall be accurate and, where necessary, kept up to date
5. **Storage limitation**
   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
6. **Integrity and confidentiality**
   Personal data shall be 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
7. **Accountability**
   The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

Personal data is information about living, identifiable individuals. It covers both facts and opinions about the individual, but need not be sensitive information. It can be as little as a name and address. Such data can be part of a computer record or manual record.

5. Notification

The General Data Protection Regulation 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 is registered.

The School will review the ICO Data Protection Register

https://ico.org.uk/ESDWebPages/DoSearch

annually, prior to renewing the notification to the Information Commissioner.

6. Privacy Notices

Whenever information is collected about individuals they must be made aware of the following:

- The identity and contact details of the data controller, e.g. the School;
- The identity and contact details of the DPO;
- The categories of pupil information we hold;
- The purpose that the information is being collected for, including the legal basis under which we are processing it;
- Any other purposes that it may be used for;
- Who the information will or may be shared with;
- Their right to request incorrect information is amended/deleted;
- Their right to remove consent to processing certain information; and
- Their right to access the information held.

This must be at the time that information first starts to be gathered on an individual.

W:\GDPR\Completed Work\Staff Privacy Notice BPAC GDPR.docx

W:\GDPR\Completed Work\Student Privacy Notice BPAC GDPR.docx

Any third party with whom data is shared must be approved by the Data Protection Officer. This is to ensure that they are compliant with GDPR and Data Protection principles in their own right and full due diligence is carried out before data is shared.

7. Conditions for Processing

Processing of personal information may only be carried out where there is a legal basis to do so (see Article 6-9).

Please see the glossary for a list of the original conditions in Articles 6-9.

8. Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- *other members of staff on a need to know basis;*
- *relevant Parents/Guardians;*
- *other authorities if it is necessary in the public interest, e.g. prevention of crime;*
- *other authorities, such as the LA and schools to which a student may move, where there are legitimate requirements (DfEE leaflet 0015/2000 entitled "Pupil Records and Reports" issued in March 2000 covers Data Protection issues and how and what information should be transferred to other schools. DfES/0268/2002 provides further information).*

The School should not disclose anything on a student's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict, advice should be obtained from the Data Protection Officer in the first instance.

When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

9. The individual's right to access their personal information (Subject Access Requests)

Any person whose details are held by the School is entitled, under the GDPR, to ask for a copy of all information held about them (or child for which they are responsible).

When a request is received it must be dealt with promptly; a response must be provided as soon as possible and within one month. The information must be provided in an electronic format when requested.

When providing the information the School must also provide a description of why the information is processed, details of anyone it may be disclosed to and the source of the data.

10. 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 13 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.

Students 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.

11. 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.

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.

12. Information Security

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. For example, possibilities may arise when computer screens are visible to the general public; files may be seen by the cleaners if left on desks overnight (all papers must be locked in cabinets when not in use).

The use of computer passwords is a requirement of the school to avoid unauthorised access. Back up discs must be kept in separate locations.

Staff who use their own devices for school related work e.g. laptops, mobile phones, USB memory sticks should familiarise themselves with, and adhere to, the Bring Your Own Device Procedures.

13. Maintenance of up to date data

Out of date information should be discarded if no longer relevant. Information should only be kept as long as needed, for legal or business purposes. In reality most relevant information should be kept for the period during which the person is associated with the School plus an additional period which the School has determined.

14. Inaccurate Data

If an individual complains that the personal data held about them is wrong, incomplete or inaccurate, the position should be investigated thoroughly including checking with the source of the information. In the meantime a caution should be marked on the person's file that there is a question mark over the accuracy. An individual is entitled to apply to the court for a correcting order and it is obviously preferable to avoid legal proceedings by working with the person to correct the data or allay their concerns.

15. Recording of Data

Records should be kept in such a way that the individual concerned can inspect them. It should also be borne in mind that at some time in the future the data may be inspected by the courts or some legal official. It should therefore be correct, unbiased, unambiguous and clearly decipherable/readable. Where information is obtained from an outside source, details of the source and date obtained should be recorded.

Any person whose details, or child's details, are to be included on the School's website will be required to give consent. At the time the information is included all such individuals will be properly informed about the consequences of their data being disseminated worldwide.

16. Photographs

Whether or not a photograph comes under the GDPR 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.

Staff with access to official school social media accounts should familiarise themselves with, and adhere to, the Social Media Procedures.

17. Breach of the policy

A breach is defined as 'a breach of security leading to the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'

Non-compliance with the requirements of the GDPR by any members of staff could lead to serious action being taken by third parties against the school authorities. Non-compliance by a member of staff is therefore considered a disciplinary matter which, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the data controller.

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

An incident includes but is not restricted to, the following:

- Accidental deletion

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad or paper record)
- Equipment theft or failure
- Systems unavailable due to power outage
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Failure to securely lock a PC when unattended
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences, where information is obtained by deceiving the organisation who holds it

18. Reporting an Incident

Any individual who accesses, uses or manages the School's information is responsible for reporting data breach and information security incidents immediately to the Data Protection Officer (DPO) (MJJones@barnwood-park.gloucs.sch.uk).

19. Retention Guidelines

The school will refer to the Information and Records Management Society (IRMS) records management toolkit for the retention guidance.

http://www.irms.org.uk/images/resources/infoguides/records_management_toolkit_for_schools_version_4_may_2012.pdf

Abbreviations

Abbreviation	Description
GDPR	General Data Protection Regulation 2018
ICO	Information Commissioner's Office
DPO	Data Protection Officer

Glossary

Data Controller	A data controller (the school is a data controller) is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.
Data Subject	The individual who the data or information is about
Educational record	The educational record is confined to information that comes from a teacher or other employee of a local authority or school, the student or their parents. Communications about a particular child from head teachers and teachers at a school and other employees at an education authority will therefore form part of that child's official educational record, as will correspondence from an educational psychologist engaged by the governing body under a contract of services. It may also include information from the child and their parents, such as information about the health of the child. Information kept by a teacher solely for their own use does not form part of the official educational record.
Information Commissioner	The independent person who has responsibility to see that the GDPR is complied with. They can give advice on data protection issues and can enforce measures against individuals or organisations who do not comply with the GDPR.

Notified Purposes	The purposes for which the school is entitled to process that data under its notification with the Office of the Information Commissioner.
Personal Data	Defined in Article 4 of the GDPR, as 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person 'the data controller' (the school is a data controller). It includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other in respect of the individual.
Processing	Covers a broad range of activities such that virtually any use of personal information or data will amount to processing.
Processed fairly and lawfully	Data must be processed in accordance with the provisions of the GDPR. These are the data protection principles, the rights of the individual and notification.
Sensitive Data	Information about racial or ethnic origin, sexual life, religious beliefs (or similar), physical or mental health/condition, biometric or genetic data, membership of a trade union, political opinions or beliefs, details of proceedings in connection with an offence or an alleged offence.
Subject Access Request	An individual's request for personal data under the GDPR.

Article 6

Lawfulness of processing

1) Processing shall be lawful only if and to the extent that at least one of the following applies:
   a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   b) 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;
   c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   e) 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 controller;
   f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2) Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3) The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

   a) Union law; or
   b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4) Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
   a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
   b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
   c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
   d) the possible consequences of the intended further processing for data subjects;
   e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Article 7

Conditions for consent

1) Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2) If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3) The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4) When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

Article 8

Conditions applicable to child's consent in relation to information society services

1) Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
   Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2) The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.
3) Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

Article 9

Processing of special categories of personal data

1) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2) Paragraph 1 shall not apply if one of the following applies:
   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. 3.

3) Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4) Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

The articles are available on the following website:
http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf