BARNSOLE PRIMARY TRUST

DATA PROTECTION POLICY

Policy reviewed by	Board of Trustees
Policy date	May 2018
Next review due	May 2020

Contents

.....

The use of **'governing board'** and **'governor'*** throughout this policy mean the accountable body for the Trust and the representatives on that body.

1. Aims

Our Trust (when referring to 'Trust' throughout this policy also refers to the schools within Barnsole Primary Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our Trust processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore are a data controller.

Barnsole Primary Trust and the schools within the Trust are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed by our Trust, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that our Trust complies with all relevant data protection obligations.

5.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the Board their advice and recommendations on Trust and school data protection issues.

The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Nicola Eckersall and is contactable via email: nicola.eckersall@bptrust.org

5.3 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that our Trust must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Trust aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Consent

Where one of the 6 'lawful bases' (legal reasons) for processing personal data does not apply generally we will ask for and will not process any personal data until consent has been obtained.

When asking for consent we will explain clearly how we will use the data, how it is stored and if it will be shared with a third party.

Where we have obtained consent to use personal data, this consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

As a general rule consent is not sought from children under the age of 12; consent will generally be sought from a parent/carer.

7.3 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the DPA. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose

for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's Records Management & Retention Policy.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Our procedures for responding to formal requests from a data subject for information that we hold about them is set out in Appendix 1

If staff receive a subject access request they must **immediately** forward it to the DPO.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.2 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must **immediately** forward it to the DPO.

10. Parental requests to see the educational record

Schools have a duty to provide an educational report annually. Parents/carers also have a legal right to access to their child's attainment and progress by submitting a written request to their child's school.

11. CCTV

We use CCTV in various locations around our school sites to ensure they remain safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the school concerned.

12. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our Trust.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

- Within schools on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing Data Protection Impact Assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

14. Data security and storage of records

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- Entry controls - any stranger seen in entry-controlled areas should be reported.

- Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential).
- Methods of disposal - paper documents should be shredded and floppy disks and CD-ROMs should be physically destroyed when they are no longer required.
- Equipment - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Trusts's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16. Personal data breaches

The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 2.

When appropriate, we will report the data breach to the ICO within 72 hours.

17. Training

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) – if any changes are made to the bill that affect our Trust's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board (this reflects the information in the Department for Education's advice on statutory policies)

19. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Information and Retention policy

Appendix 1

Procedure for Subject Access Requests

1. Making a subject access request

An individual is only entitled to access their own personal data, and not to information relating to other people. Individuals with parental responsibility may make requests for personal information relating to their child, unless we determine that the child has the capacity to make their own decisions about their personal information. In these circumstances, we will discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their personal data.

For a subject access request to be valid, it must be made in writing e.g. letter, email or fax. It is helpful if the person requesting the information identifies the request as a subject access request and addresses the request to the Data Protection Officer.

The request must be sufficiently detailed to enable us to identify and find the personal data covered by the request. If we are unsure, we can request further information. Until this further information is received, we do not need to comply with the subject access request.

We will provide the information free of charge.

We are also entitled to request information to judge whether the person making the request is the individual to whom the personal data relates and/or is a person with parental responsibility for a child whose data is the subject of the request. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception. Evidence of identity may be established by production of:

- passport
- driving licence
- utility bills with the current address
- birth / marriage certificate
- P45/P60
- credit card or mortgage statement

2. Responding to a subject access request

The response time for subject access requests, once officially received, is within 1 month of receipt of the request (irrespective of school holidays).

We may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

When responding to a subject access request, we will:

a. acknowledge receipt of the request and provide an indication of the likely timescale for a response within 5 working days;
b. take all reasonable and proportionate steps to identify and disclose the data relating to the request;
c. never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events;
d. consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;
e. seek legal advice, where necessary, to determine whether we are required to comply with the request or supply the information sought;
f. provide a written response, including an explanation of the types of data provided and whether and for what reasons any data has been withheld; and
g. ensure that information disclosed is clear and technical terms are clarified and explained.

3. Circumstances where we may refuse a subject access request

We are not required to comply with a subject access request in relation to:

a. confidential references given by us for employment or educational purposes;
b. personal data processed in connection with management forecasting or planning if it would prejudice the conduct of the business of the Academy;
c. personal data subject to legal professional privilege; or
d. information which may cause serious harm to the physical or mental health or emotional condition of a child or another, or which would reveal that a child is at risk of abuse, or information relating to court proceedings.

We are also not required to supply the information requested if:

a. the data requested is not available;
b. it would involve disproportionate effort to disclose the information requested;
c. an identical or similar request has been made by the same individual previously, unless a reasonable interval has elapsed between the previous and the current request; in determining whether a 'reasonable interval' has elapsed, we will have regard to the nature of the data, the purpose for which the data is processed and the frequency with which the data is altered;
d. we cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless:

    (i) the other individual has consented to the disclosure of the information, or
    (ii) it is reasonable in all the circumstances to comply with the request without the consent of the other individual; in determining whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, we shall have regard shall be had to any duty of confidentiality owed to the other individual and any express refusal of consent by the other individual.

In order to provide the whole or some of the information requested, we may undertake redaction (information blacked out/removed) of one or more documents. An explanation of why we have redacted the information will be provided.

Appendix 2

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must **immediately** notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The DPO will alert the Chief Executive Officer and the Head teacher.
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
    - Facts and cause
    - Effects
    - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
- The DPO, Chief Executive Officer and Head teacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Procedures to minimise the impact of data breaches

We will put in place procedures and systems to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these procedures and systems and amend them as necessary after any data breach.