Data Protection Policy

BASSETT GREEN
PRIMARY SCHOOL

Policy written by:	Elizabeth Davies
Approved on:	10/09/2024
Review date:	01/07/2025
Added to the school website?	Yes

Data Protection Policy

Contents Page

1 School Vision

Bassett Green Primary School is defined by its ethos to place each child at the heart of all that we do. We are committed to creating an environment that ensures equality of opportunity for every child. We know that children thrive in positive and happy environments in which there are clear and agreed expectations and boundaries. It is this culture that underpins our policies and procedures. All members of the School family – staff and pupils are governed by our policies. We all abide by the same codes of conduct and act respectfully to each other.

2 Policy Aims

This policy statement covers the uses of personal information about current, past and prospective staff, pupils, parents and other individuals who come into contact with the school. All school staff and governors involved with the collection, use, processing or disclosure of personal data will be aware of their duties and responsibilities and will adhere to this policy.

Personal data may be collected and used in order to meet legal requirements and legitimate interests set out in Data Protection Legislation, namely:

- The General Data Protection Regulation (Regulation (EU) 2016/679)
- The Law Enforcement Directive (Directive (EU) 2016/680)
- The Data Protection Act 2018
- All applicable law about the processing of personal data and privacy.

This information is collected, used and stored to enable the provision of education and other associated functions. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of the government. The personal information will be dealt with in line with Data Protection Legislation regardless of the way that it has been collected, recorded and used.

The policy is in line with Southampton Local Authority guidelines.

3 Why is it necessary?

Bassett Green Primary School is registered as a Data Controller, with the Information Commissioner's Office (ICO), and its registration number is A8426564. Details are available on the ICO website: https://ico.org.uk/edswebpages/search

The personal data is used for the following reasons:
- To support pupil learning
- To monitor and report on pupil progress
- To provide appropriate pastoral care
- To assess the quality of our service
- To comply with the law regarding data sharing
- To safeguard pupils

4 What information is collected?

All data within the school's control shall be identified as personal, sensitive, or both, to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

Data Protection Legislation applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. Data Protection Legislation refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

The information collected includes contact details, national curriculum assessment results, attendance information and personal characteristics, such as ethnicity, any special educational needs, and relevant medical information.

The categories of pupil information that we collect, hold and share include:

• Personal information (such as name, unique pupil number and address)
• Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
• Attendance information (such as sessions attended, number of absences and absence reasons)
• Academic progress/assessment data
• Relevant medical information
• Special educational needs information
• Exclusions/behavioural information

Our school regards the lawful and correct treatment of personal information as very important to the successful maintenance of confidence between individuals and ourselves. We ensure that personal information is treated lawfully and correctly.

To this end, we fully endorse and adhere to the six principles of data protection, as detailed in the Data Protection Legislation.

5 Data Protection Principles

Under Data Protection Legislation, there are six data protection principles that set out the main responsibilities for organisations, including schools.

Personal data shall be:

• **Principle 1**: processed lawfully, fairly and in a transparent manner in relation to individuals.
Principle 2: collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

• **Principle 3**: adequate, relevant and limited to what is necessary.

• **Principle 4**: 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.

• **Principle 5**: 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.

• **Principle 6:** processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.

As the data controller, the school is responsible for, and must be able to demonstrate compliance with these principles.

6 Obligation

The school is committed to maintaining the above principles at all times. Therefore the school will:

• Observe fully the conditions regarding the fair collection and use of information.

• Meet its legal obligations to specify the purposes for which information is used.

• Collect and process the appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

• Ensure the quality of information used is accurate and kept up-to-date.

• Apply strict checks to determine the retention periods of information held.

• Guarantee the rights of people about whom information is held can be fully exercised under Data Protection Legislation (these include the right to be informed that processing is being undertaken); ensure the public have the right of access to personal records held about them.

• Ensure individuals have the right to access one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information

• Ensure that for all personal data, appropriate security measures are taken, both technically & organisationally, to protect against damage, loss or abuse.

• Ensure that personal information is not transferred abroad without suitable safeguards.

• Adopt the key principles of BS7799 – the British Standard on Information Security Management.

• Regularly review this Policy and safeguards that relate to it to ensure that the contents are still relevant, efficient and effective.

• Ensure CCTV systems are used in compliance with Data Protection Legislation.

• Adhere to the duty of confidence.

• Everyone managing and handling personal information understands that they are responsible for following good data protection practice and are appropriately trained to do so.

• Queries about handling personal information are promptly and courteously dealt with.

7 Fair processing (Sharing personal data)

We shall be transparent and provide accessible information about the proposed processing of data and communicate these intentions via notification to staff, parents and pupils.

We do not share information about our pupils with anyone without consent, unless the law and our policies allow us to do so.

We share pupils' data with Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.
We are required to share information about our pupils with Southampton City Council (SCC) and the DfE under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

We also share pupil information to:
• Meet our statutory duty to create and maintain an admission register under the Education (Pupil Registration) (England) Regulations 2006 and subsequent amendments, without which schools are unable to enrol a pupil.

• Support teaching and learning. In order to facilitate this, we may share information with the software supplier to set up the systems needed for pupils and parent/carers to access.

• Monitor and report on academic progress.

• Provide appropriate pastoral care (Keeping Children Safe in Education 2020).

• Assess how well we, as an education provider, are doing.

• Co-operate with SCC and external partners to improve the wellbeing of children, under the duty of the Children Act 2004.

• Share information with SCC and external partners to support the duty to safeguard and promote the welfare of children, under the Children Act 1989, Section 17.

• Share data with professionals commissioned by the school or working with a pupil such as the School Nurse or health services.

Comply with our statutory duty under the Education (Pupil Information)(England) Regulations 2005 Statutory Instrument and subsequent amendments in The Education (Pupil Information) (England) (Amendment) 2008 to create a Common Transfer File when a child ceases to be registered at a school and becomes a registered pupil at another school in England or Wales. This would also apply to pupils who are dually registered at more than one school. If a Common Transfer File cannot be sent to a new school when a pupil leaves, one must be sent to the DfE Lost Pupil Database.

• Provide information via statutory census returns to the DfE and in turn this will be available for the use of SCC to carry out its official functions, or a task in the public interest. Further information can be found online at https://www.gov.uk/government/publications/schoolcensus-2016-to-2017guide-for-schools-and-las

• Send pupil information to SCC on a regular basis in accordance with our information sharing agreement to enable the local authority to meet its duty under Data Protection Legislation to ensure that the data it holds is accurate and also to carry out its official functions, or a task, in the public interest.
• Notify SCC on a termly basis of all pupils on a reduced timetable so that the local authority can comply with statutory Ofsted requests for data at the time of inspection.

• Comply with the statutory requirements of the Education (Pupil Registration) (England) Regulations 2006 and subsequent amendments, notifying SCC if a child leaves the school and providing forwarding details. A failure to provide this information will result in pupils being recorded as a “Child Missing Education”, in accordance with the government definition.

• Provide attendance information to SCC so that its duties under the Anti-Social Behaviour Act 2003, Section 444 of the Education Act 1996 and Section 36 of the Children Act 1989 (Education Supervision Orders) can be met.

• Provide exclusion information to SCC so that its duty Under Section 19 of the Education Act 1996 can be met.

• Meet our duty to provide information about any exclusions with the last 12 months to the Secretary of State and (in the case of maintained schools and PRUs) the local authority, in accordance with The Education (Information about Individual Pupils) (England) Regulations 2006.

When your child applies for further education or training, the school/SCC may forward information to colleges or providers in order to aid your child’s transition into further education or training.

There shall be restricted access to personal information, giving access only to people (staff and governors) who need particular information to do their job, and only when they need it. This covers access to written and electronic staff and pupil records, and recorded CCTV images. Any proposed change to the processing of individual’s data shall first be notified to them.

8 Photography and media footage

Images of staff and pupils may be captured at suitable times and as part of educational activities for use in school only. Any images will only be used for the purpose that has been specified.

In the event that an education organisation decides to use surveillance technology, i.e. CCTV and body-worn video, it will be done in line with current Data Protection Legislation.

Individuals will be made aware they may be recorded and appropriate measures will be put in place to keep the recorded images secure.

9 Data security, storage and disposal of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- 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 school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

10 Personal data breaches

The school 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 1.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

11. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every **2 years** and shared with the full governing board.

12. Subject access requests and other rights of individuals

12.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

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

12.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

12.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity, where relevant)
- Will provide the information free of charge
- 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

We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

12.4 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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.

13 Training

All staff and governors are provided with data protection training on an annual basis. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

14 Further information

If you wish to be supplied with personal information we hold about you (a subject access request), please make a request addressed to the School's Data Protection Officer.

Complaints will be dealt with in accordance with the school's Complaints Policy.

If you have any concerns or queries about how the school is processing your personal data, please contact the school's Data Protection Officer, **Elizabeth Davies**:
Bassett Green Primary School, Honeysuckle Road, Southampton SO16 3BZ
Tel: 023 8067 6262, Email: info@bassettgreen.net

For independent advice about data protection, please contact the **Information Commissioner**
Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545 745 (national rate number)
Email: casework@ico.org.uk

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

- On finding or causing a breach, or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by emailing info@bassettgreen.net
- 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
- Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation
- If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers). (See the actions relevant to specific data types 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 before and after the implementation of steps to mitigate the consequences
- The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool

- The DPO will document the decisions (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. 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 of the school's awareness of the breach. 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
- Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
    - A description, in clear and plain language, of the nature of the personal data breach
    - 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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)

Records of all breaches will be stored on the school's computer system.

- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible
- The DPO and headteacher will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error

- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error

- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the [ICT department/external IT support provider] to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)

- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way

- The DPO will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to

request that the information is removed from their website and deleted

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners

Other types of breaches include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen
- Hardcopy reports sent to the wrong pupils or families