

Data Protection Policy Statement

(including Biometric Data)

1. Policy Statement

The Governing Body of Bridgnorth Endowed School has overall responsibility for ensuring records are maintained, including security and access arrangements, in accordance with Education Regulations and all other statutory provisions.

The staff of Bridgnorth Endowed School recognise the importance of following the principles of the Data Protection Act 1998 and making sure that information is securely and appropriately managed.

The Headteacher and Governors of this school intend to comply fully with the requirements and principles of the Data Protection Act 1998. All staff involved with the collection, processing and disclosure of personal data are aware of their duties and responsibilities within these guidelines.

Bridgnorth Endowed School is required to process relevant personal data regarding staff, pupils, their parents and guardians. We shall take all reasonable steps to do so in accordance with this policy. Processing may include obtaining, recording, holding, disclosing, destroying or otherwise using data. Reference to pupils in this policy includes current, past or prospective pupils.

2. Aims & Objectives

The school shall so far as is reasonably practicable comply with the eight Data Protection Principles contained in the Data Protection Act to ensure all data is:

1. Obtained and processed fairly and lawfully
2. Processed for specified, lawful purposes
3. Adequate, relevant and not excessive
4. Accurate and kept up to date
5. Not kept for longer than necessary
6. Processed in accordance with the individual's legal data rights
7. Securely protected against unauthorised processing, accidental loss, destruction or damage
8. Not transferred to other countries (especially outside the EU) without adequate protection

The school shall also under the new Protection of Freedoms Act 2012 (sections 26 to 28), the school is required to notify each parent of a child and obtain the written consent of at least one parent before being able to use a child's biometric information for an automated system.

3. Responsibilities

The Data Protection Controller

The key person at Bridgnorth Endowed School is the Data Protection Controller (Director of Business & Finance). This person is required to undergo training as necessary, to make sure that the procedures in this policy are followed, and to provide detailed guidance where required. The Data Protection Controller will seek to ensure that all personal data is processed in compliance with this Policy and the Principles of the Data Protection Act 1998. Data protection procedures will be followed by all staff members.

4. Implementation

4.1 Personal Data

Definitions of personal data are highly complex, and it is difficult to define categorically. However, broadly speaking and in day-to-day use, 'personal data' is information which relates to a living, identifiable individual.

In the context of this document and the School's requirement to process 'personal data' as part of its duty of care and to educate its pupils, 'personal data' may include:

- School admission and attendance registers
- Pupil's curricular records
- Reports to parents on the achievements of their children
- Records in connection with pupils entered for prescribed public examinations
- Staff records, including payroll records
- Pupil disciplinary records
- Personal information for teaching purposes
- Records of contractors and suppliers

The data we hold at Bridgnorth Endowed School is as follows:

How held	What type of system	Where stored
Manual / computerised SIMS	Pupils academic records	School office / IT network
Manual / computerised SIMS	Class lists	School office / IT network
Manual / computerised SIMS	Staff Personnel files	Head's records / IT network
Computerised SIMS	Attendance module	IT network
Computerised SIMS	Personnel module	IT network
Manual / computerised SIMS	Pupil personal data	School office / IT network
Computerised NRS	Biometric system – meals / printing system	IT network
Computerised MicroLibrarian	Biometric system – library	IT network

4.2 Biometric Data

Biometric Information and how it will be used

Biometric Information is information about a person's physical or behavioural characteristics than can be used to identify them, for example, information from their fingerprint.

Bridgnorth Endowed School would like to use information from a person's fingerprint and use this information for the purposes of providing access to the library, catering and printing facilities of the school.

The information will be used as part of an automated biometric recognition system. This system will take measurements of a fingerprint and convert these measurements into a template to be stored on the system. An image of fingerprint is **not** stored. The template (i.e. measurements taking from a fingerprint) is what will be used to permit access to services.

It should be noted that the law places specific requirements on schools when using personal information, such as biometric information, about pupils for the purposes of an automated biometric recognition system.

For example:

- a) The school cannot use the information for any purpose other than those for which it was originally obtained and made known to parents i.e. as stated above;
- b) the school must ensure that the information is stored securely;
- c) the school must inform what it intends to do with the information;
- d) unless the law allows it, the school cannot disclose personal information to another person/body – it is noted that the only person / body that the school wishes to share the information with is Nationwide Retail Systems, Micro Librarian Systems. This is necessary in order to manage the system and will be handled under the guidelines of the data protection act.

Providing consent / objecting

As stated above, in order to be able to use biometric information, the written consent of at least one parent is required. However, consent given by one parent will be overridden if the other parent objects in writing to the use of their child's biometric information. Similarly, if a child objects to this, the school cannot collect or use his / her biometric information for inclusion on the automated recognition system.

Parents / staff can also object to the proposed processing of your biometric information at a later stage or withdraw any consent that has previously been given. Please note that any consent, withdrawal of consent or objection from a parent must be in writing.

Even if a parent has consented, a child can object or refuse at any time to their biometric information being taken / used. His / her objection does not need to be in writing.

The law says that schools must provide reasonable alternative arrangements for children who are not going to use the automated system to access the library, catering and printing

facilities, Bridgnorth Endowed School provide PIN numbers for all who do not wish to use the biometric systems.

When a child leaves the school, or if some other reason he / she ceases to use the biometric system, his / her biometric data will be securely deleted.

4.3 Processing Personal Data

The data is used by authorised members of the schools' staff to support the legitimate interests of the schools, i.e. the provision of education. Relevant parts of the data may be disclosed legitimately to authorised personnel within the school, health advisers, social workers and other relevant agencies, to prospective employers and to the data subjects themselves. Data processing is done internally by authorised school staff and externally the Shropshire Local Authority.

If it is necessary for the school to process certain personal data to fulfil its obligations to pupils and their parents or guardians then consent is not required. However, any information which falls under the definition of personal data, and is not otherwise exempt (see part 8), will remain confidential. Data will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this Policy.

4.4 Sensitive Personal Data

'Sensitive data' may include:

- Ethnic or racial origin
- Political opinions
- Religious beliefs
- Other beliefs of a similar nature
- Membership of a trade union
- Physical or mental health or condition
- Sexual life
- Offence or alleged offence
- Proceedings or court sentence

Where sensitive personal data is processed by the school, the explicit consent of the appropriate individual will be required in writing.

4.5 Rights of Access

Individuals have the right of access to information held by the school. Any individual wishing to access their personal data should put their written request to the Data Protection Controller. The school will try to respond to any such written requests as soon as is reasonably practicable and in any event, within 40 days for access to records and 21 days to reply to an access to information request.

Parents and guardians do have right of access to their child's educational record. They should make the request in writing to the **Director of Business & Finance**.

It is important to note that certain data is exempt from the right of access under the Data Protection Act. This can include:

- Information which identifies other individuals
- Information which the school reasonably believes would be likely to cause serious harm to the physical or mental health or emotional condition of the pupil or someone else
- Information concerning actual or suspected child abuse
- Reports by the school to a juvenile court
- Information which is subject to legal professional privilege
- Pupil examination scripts

The school will also treat as confidential any reference given by the school for the purpose of the education, training or employment, or prospective education, training or employment of any pupil. The school acknowledges that an individual may have the right to access a reference relating to them received by the school. However such a reference will only be disclosed if doing so does not identify the referee or where, notwithstanding this, the referee has given their consent or if disclosure is considered reasonable.

4.6 Data Rights

Under the Data Protection Act, the rights of the data belong to the individual to whom the data relates. However, in most cases, the school will rely on parental consent to process data relating to pupils unless, given the circumstances and the pupil's age and understanding, it is unreasonable to rely on the parent's consent. Parents should be aware that in such situations they may not be consulted. These situations are very rare, and it is a general policy in the school to always seek parental or guardian consent before processing a child's personal data.

The school is legally required to give a pupil access to their personal data if in the school's reasonable belief the pupil understands the nature of the request and its implications. However, it should be noted that in accordance with Section 30 of the Exemptions to the Data Protection Act 1998, if the school does not consider it appropriate for a pupil to see a particular document which a pupil has asked to see and even obtained a parental request for access to that data, the school can withhold access.

Where a pupil seeks to raise private concerns confidentially with a member of staff and makes it clear they do not want the data passed on to their parents or guardian, the school will maintain confidentiality unless it has reasonable grounds to believe the pupil does not fully understand the consequences of withholding their consent, or where the school believes disclosure will be in the very best interests of the pupil or other pupils.

4.7 Exemptions

Certain data is exempted from the provisions of the Data Protection Act:

- The prevention or detection of crime
- The assessment of any tax or duty
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the school

There are other exemptions under the Act. Requests for further information on exemptions should be made to the School Data Protection Controller.

4.8 Disclosure of Information

The school confirms that it will not generally disclose information about individuals, unless the individual has given their consent or one of the specific exemptions under the Data Protection Act applies. However, for the following purposes, the school does intend to disclose data as is necessary to third parties:

- To give confidential references for any educational institution which the pupil may wish to attend
- To give information relating to outstanding fees or payment history to any educational institution which it is proposed that the pupil may attend
- To publish the results of public examinations or other achievements of pupils of the school
- To disclose medical details of a pupil's medical condition where it is in the pupil's interest to do so (eg. To organisers of a school trip).

When the school receives a disclosure request from a third party it will always take action to establish the identity of that third party before making any disclosure.

4.9 Use of personal Information by the School

As part of the entry procedure into the school at any age, all pupils are asked to sign an agreement giving the school their consent to use their personal data for:

- Use of photographic images in school publications (eg. BEST or on the school website)
- Fundraising, marketing or promotional purposes and to maintain relationships with pupils of the school

4.10 Accuracy

In accordance with the Data Protection Act 1998 it is school policy to ensure that any personal data held about an individual is accurate. Conversely, the school will seek to encourage all pupils and staff to notify the Data Protection Controller of any changes to information held about them (change of address, change of marital status etc). The school recognises the individual right to request that inaccurate information about them is erased or corrected.

Bridgnorth Endowed School sends home a form annually for parents to update the details held in SIMS (name, address, contact details, emergency contacts etc) to ensure accuracy.

4.11 Security

Where it is reasonably practicable, the school will take steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this policy and their duties

under the Data Protection Act. The school will ensure that all personal information is held in a secure central location and is not accessible to unauthorised persons.

Electronic data is stored on the computer network. This is password protected and access rights are restricted to authorised personnel. The data is backed up every night. Computer screens are sighted so that they are not easily seen by visitors to the office, and password screen savers are used to increase security.

4.12 Electronic transmission of data

Bridgnorth Endowed School has moved largely towards electronic transmission as the main method of data transfer. The School Census is transmitted electronically, teaching staff are increasingly using electronic means (SIMS assessment module) to record pupil assessments, and transfers of data to other schools are via the School to School website.

E-mail has become an increasingly common method of communication. Staff are urged to delete unread e-mails from unknown sources and with irrelevant subject headings in order to minimise the risks of virus transmission. Pupil data is transferred to Shropshire LA, when necessary, by secure file transfer.

Anti-virus software is installed on the network and is updated regularly. Data held on paper is stored in either / and locked filing cabinets or locked offices.

4.13 Disposal of Data

Records are destroyed when no longer relevant, paper formats by shredding, with the constraints detailed within the Retention Guidelines.

4.14 Enforcement

If an individual believes that the school has not complied with this policy or acted otherwise than in accordance with the Data Protection Act, they should make a complaint to the school and notify the Data Protection Controller.

5. Monitoring

- The Director of Business & Finance (Data Controller) will ensure that data protection requirements and requests are handled according to this policy.
- All Data Protection queries will be forwarded to the Director of Business & Finance; all will be recording and reported to the Governors Compliance & Risk Committee
- This policy will be reviewed annually and / or when any legislation should change
- All staff will have access to the most up to date Retention Guidelines and must refer to these when disposing of any documentation