Data Protection Policy

The Data Protection Act 1998 is the law that protects personal privacy and upholds individuals' rights. It applies to anyone who handles or has access to people's personal data. This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act. It will apply to information regardless of the way that information is used, recorded and stored and whether it is held in paper files or electronically.

The **Data Protection Act 2018** achieved Royal Assent on 23 May 2018 and implements the government's manifesto commitment to update the UK's data protection laws - **General Data Protection Regulation (GDPR**). Bright Futures School Data Protection Policy now reflects the 2018 Act and also takes account of the schools' Privacy notices. **GDPR** alters how businesses and public sector organisations can handle the information of their customers. It also boosts the rights of individuals and gives them more control over their information.

The main elements of the **2018 Act** are:

General data processing:

● Implements GDPR standards across all general data processing.

● Provides clarity on the definitions used in the GDPR in the UK context.

● Ensures that sensitive health, social care and education data can continue to be processed while making sure that confidentiality in health and safeguarding situations is maintained.

● Provides appropriate restrictions to rights to access and delete data to allow certain processing currently undertaken to continue where there is a strong public policy justification, including for national security purposes.

● Sets the age from which parental consent is not needed to process data online at age 13, supported by a new age-appropriate design code enforced by the Information Commissioner.

Law enforcement processing:

● Provides a bespoke regime for the processing of personal data by the police, prosecutors and other criminal justice agencies for law enforcement purposes.

● Allows the unhindered flow of data internationally whilst providing safeguards to protect personal data.

Intelligence services processing:

● Ensures that the laws governing the processing of personal data by the intelligence services remain up-to-date and in-line with modernised international standards, including appropriate safeguards with which the intelligence community can continue to tackle existing, new and emerging national security threats.

Regulation and enforcement:

● Enacts additional powers for the Information Commissioner who will continue to regulate and enforce data protection laws.

● Allows the Commissioner to levy higher administrative fines on data controllers and processors for the most serious data breaches, up to £17m (€20m) or 4% of global turnover for the most serious breaches.

● Empowers the Commissioner to bring criminal proceedings against offences where a data controller or processor alters records with intent to prevent disclosure following a subject access request.

Purpose

Personal information is any information that relates to a living individual who can be identified from the information. This includes any expression of opinion about an individual and intentions towards an individual. It also applies to personal data held visually in photographs or video clips or as sound recordings.

The school collects a large amount of personal data every year including: staff records, names and addresses of those enquiring about places at the school, references, volunteer details etc. This information is gathered in order to enable the provision of education and other associated functions. Personal data includes (but is not limited to) an individual's name, address, date of birth, photograph, bank details and other information that identifies them. In addition, the school may be required by law to collect and use certain types of information to comply with statutory obligations of the Local Authority, government agencies and other bodies.

All school staff 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.

The Eight Data Protection Principles

The Data Protection Act 1998 is based on eight data protection principles, or rules for 'good information handling':

1. Data must be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specific and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
4. Personal data shall be accurate and where necessary kept up to date.
5. Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose.
6. Personal data shall be processed in accordance with the rights of data subjects under the 1998 Data Protection Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Responsibilities

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. **Bright Futures School** is registered as a Data Controller and as such have issued a Privacy Notice to all pupils/parents, this summarises the information held on pupils, why it is held and the other parties to whom it may be passed on. The privacy notice can also be found on the school website.

The school must:

• Manage and process personal data properly
• Protect the individual's right to privacy
• Provide an individual with access to all personal data held on them (as identified in the privacy notice)

Commitment

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

The school will:
• Inform individuals why personal information is being collected.
• Inform individuals when their information is shared, and why and with whom unless the Data Protection Act provides a reason not to do this.
• Check the accuracy of the information it holds and review it at regular intervals.

• Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
• Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
• Ensure that personal information is not retained longer than it is needed.
• Ensure that when information is destroyed that it is done so appropriately and securely.
• Share personal information with others only when it is legally appropriate to do so.
• Comply with the duty to respond to requests for access to personal information, known as Subject Access Requests.
• Ensure that personal information is not transferred outside the EEA without the appropriate safeguards
• Ensure all staff and managers are aware of and understand these policies and procedures.

Data retention

- Organisations must not keep personal data for longer than you need it.
- Organisations need to think about – and be able to justify – how long you keep personal data. This will depend on your purposes for holding the data.
- Our standard retention periods are set out below. These comply with documentation requirements.
- We will also periodically review the data we hold, and erase or anonymise it when we no longer need it.
- We must carefully consider any challenges to your retention of data. Individuals have a right to erasure if we no longer need the data.
- Organisations can keep personal data for longer if they are only keeping it for public interest archiving, scientific or historical research, or statistical purposes.

Our data retention periods for different data are set out in our data retention policy.

Complaints

Any member of staff, parent or other individual who considers that the policy has not been followed, in respect of personal data about themselves or their child, should raise the matter with the Head of Learning in the first instance. Complaints relating to the handling of personal information may be referred to the Information Commissioner @ www.ico.gov.uk or **0303 123 1113.**

Review

This policy will be reviewed by school management as deemed necessary but at least every two years.

Agreed: October 2017, updated October 2018, November 2019, January 2021, January 2022; January 2023; January 2024; July 2024. Next Review July 2025

Appendix 1

Bright Futures School.
Procedures for responding to subject access requests made under the Data Protection Act 2018

Rights of access to information
Under the Data Protection Act 2018 any individual has the right to make a request to access the personal information held about them.

These procedures relate to subject access requests made under the Data Protection Act 2018.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to Zoe Thompson. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However, with children, this is dependent upon their capacity to understand (age 13 or above) and the nature of the request. The Head of Learning / Development should 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 records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:

- Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.
- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the School.

School has developed guidelines for managing SARs which should be read in conjunction with this policy.