Baden Powell

Data Protection Policy

Approved by:	Insert details of DPO or school data protection lead
Last reviewed on:	Sepetember 2022
Next review due by:	September 2024

Document contents:

1. Definitions

The school	means [insert school name]
GDPR	means the General Data Protection Regulation.
Personal Data	means data which relates to a living individual. That individual must be identified or identifiable either directly or indirectly from one or more identifiers or from factors specific to the individual.
Special Category Data	means specific information about an individual that relates to their race or ethnic background; political opinions; religious beliefs; trade union membership; health; sexual health; sexual orientation; criminal records.
DPA	means the Data Protection Act 2018.
Data Controller	means the organisation that decides how the personal data is processed. For the purposes of this policy the data controller is the school.
Data Processor	means any organisation a data controller shares personal data with for a specified purpose. What they can and cannot do with that personal data is decided by the data controller.
Data Subject(s)	means staff/potential staff/former staff, pupils and their families, former pupils and their families, or any other living individuals whose personal data may be processed by the school.
Data processing	means anything the school does with the personal data from the point of collection to the date of its destruction. Simply holding data is still data processing.
Data Protection Officer	means the designated person appointed as Data Protection Officer in accordance with Article 37 of the GDPR.
Information Asset Register	means a register of all data processing activities and systems or contexts in which personal data is processed by the school.
Privacy Notice	means a document that explains to data subjects what we do with their personal data and why. It also explains our lawful basis for doing so and sets out what rights they have with regard to their personal data.
ICO	means the Information Commissioner's Office, being the supervisory authority responsible for enforcing the DPA.

2. Aims and Purpose of this Policy

The school collects, uses, stores and otherwise processes personal data relating to staff (and potential staff), pupils and their families, former staff and former pupils. *All of the people to whom personal data held by the school relates are collectively referred to in this policy as data subjects.*

This policy sets out how the school aims to meet its responsibilities as a data controller and to ensure that all personal data is processed in accordance with the requirements of the General Data Protection Regulation and Data Protection Act 2018.

This policy therefore seeks to ensure that we:

- are clear about how personal data must be processed and the school's expectations for all staff who process personal data on its behalf;
- comply with data protection law and any other identified best practice;
- protect the rights and freedoms of all data subjects
- protect the school's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
- protect the school from risks of personal data breaches and other breaches of data protection law.

3. Roles and Responsibilities

This policy applies to all staff employed by the school and to any external organisations or individuals who may process personal data on its behalf.

3.1. The Governing Body

The Governing Body has overall responsibility for the school's compliance with the GDPR, DPA and any relevant information legislation.

3.2. The Headteacher

The Headteacher will act as the representative of the data controller on a day-to-day basis. This means they will make decisions in relation to data protection matters as required, consulting the Governing Body and taking advice from the Data Protection Officer if required.

3.3. The Data Protection Officer (DPO)

The DPO shall take responsibility for overseeing the implementation of this policy and monitoring the school's compliance with the GDPR, DPA and any relevant information legislation.

The DPO shall act as the first point of contact for any data subjects and for the ICO.

The Data Protection Officer shall not be held personally responsible for the school's compliance with the GDPR and Data Protection Act 2018.

The DPO is **Marsha Mollienux at MMollineux@baden-powell.hackney.sch.uk**

3.4. All staff

All staff are responsible for:

- ensuring data is collected, stored and otherwise processed in accordance with this policy
- keeping records relating to themselves (address, contact details) up to date
- contacting the DPO if they have they have any queries relating to this policy and their responsibilities under it, to report a data breach or any suspected data breach, to notify the DPO of any new activity that may involve data processing and to discuss any contracts with or data sharing requests from third parties.
- contacting the DPO if they receive a subject access request (see section 5)

4. Data protection principles

The school is committed to processing personal data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR states that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. 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;
e. 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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."

5. Lawful, fair and transparent processing

5.1. Personal data processed by the school must be done on one of the following lawful bases listed in Article 6 of the GDPR. This means the school will only process personal data where;

- it is necessary for the school, as a public authority, to perform its official functions identified as **public interest tasks**;
- it is necessary in order for the school to comply with a **legal obligation**;
- it is necessary for the school to fulfil a **contractual obligation** with the individual;
- it is necessary to protect a data subject's **vital interests**, e.g. sharing information about their health with emergency services;
- it is necessary for the school's **legitimate interests** (ensuring any data subject's rights and freedoms are not compromised);
- where the parent/carer or pupil (if appropriate) has freely given clear affirmative **consent**

5.2. Special category data processed by the school must be processed on one of the following lawful bases listed in Article 9 of the GDPR. This means special category data will only be processed where;

- it is necessary for the performance of a substantial public interest task;
- it is necessary for the school to ensure compliance with employment and social security law;
- it is necessary to protect the vital interests of a data subject

5.3. The school will issue a privacy notice whenever personal data is collected from individuals for the first time. Privacy notices will explain our lawful basis for processing the data, how it will be used and what rights those individuals have in relation to it.

5.4. To ensure its processing of data is lawful, fair and transparent, the school shall maintain an Information Asset Register. The school shall note the appropriate lawful basis for all data processing activities in the Information Asset Register.

5.5. The Information Asset Register shall be reviewed at least annually.

5.6. Where consent is relied upon as a lawful basis for processing data, evidence of affirmative opt-in consent shall be kept with the personal data. Data subjects will be notified that they can withdraw their given consent to process their personal data at any time.

5.7. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent will be made available and systems put in place to ensure such revocation is reflected accurately in the school's records.

6. Data Limitation, Minimisation and Accuracy

6.1. The school shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6.2. The school will not collect any personal data that is not required for the purposes described to the data subject at the point of collection or in the school's Privacy Notice.

6.3. The school must only process personal data where it is necessary to fulfil its public tasks, meet a legal or contractual obligation, protect an individual's vital interests, serve the school's legitimate interests or where clear consent is freely provided.

6.4. When the personal data is no longer needed to fulfil its purpose, or where there is no clear lawful basis for processing it, staff must ensure the data is deleted or anonymised in accordance with the Retention Schedule**.**

7. Data Subjects' Rights

Individuals have various rights in relation to their personal data. Data subjects shall be notified of their rights in the school's privacy notice. Any requests made to the school in relation to these rights shall be dealt with in a timely manner.

7.1. Subject Access

Individuals have a right of access to personal information the school holds about them. They can access this information by making a subject access request. They can request:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- An explanation of the purposes of the data processing
- The categories of personal data concerned
- Who the data is shared with
- How long the data will be stored for
- How the school received the data (if not from the individual making the request)
- Whether any automated decision making processes are applied to their data and how this may affect them

Subject access requests should include:

- The name of the individual
- A valid correspondence address
- Details of the information they are requesting

7.2. The school will respond to a subject access request within one month of receiving it.

7.3. Any school staff who receive a subject access request must notify the DPO as soon as possible

7.4. Where necessary, the school will request that data subjects provide 2 forms of identification to ensure information is not disclosed to a third party. Staff should only request this if there is reasonable doubt as to who is making the subject access request.

7.5. The school will not charge a fee for processing a subject access request unless it is manifestly unfounded or excessive, in accordance with relevant ICO guidance. A request will be deemed unfounded or excessive if it is repetitive or simply asks for further copies of the same information.

7.6. The school may contact the data subject to notify them we will comply within 3 months of receipt if the request is complex. The school will notify the data subject within 1 month of receipt of the request and explain why an extension is necessary.

7.7. The school will not disclose the information if an exemption listed in schedules 2-4 of the DPA are engaged. If refusing a request the school will write to the data subject to explain why and notify them of their right to complain to the ICO.

7.8. The school will consider any risk of causing serious harm to the physical or mental health of pupils or any other individuals as a result of disclosing personal information in response to a subject access request. Upon careful consideration the school may choose not to disclose information if there is a significant risk of causing serious harm or distress as described above.

7.9. Personal data about a child belongs to that child as an individual rather than to their parents or carers. For a parent or carer to make a valid subject access request for data relating to their child, the child must either be unable to understand their rights in relation to their personal information or otherwise have freely given their consent. Children below the age of 12 are generally not regarded to be competent in terms of understanding their rights and the implications of a subject access request. Therefore, requests from parents or carers of pupils under 12 years of age may be granted without obtaining the explicit and freely given consent of the pupil.

7.10. Subject access requests from parents or carers of pupils 12 years of age or older may require the freely given consent of the pupil depending on their competence in terms of understanding their rights in relation to their personal data. School staff must consider obtaining the consent of any individuals 12 years of age or older on a case-by-case basis.

7.11. Other rights under GDPR

In addition to the right of subject access, individuals also have a right to;

- withdraw their consent to processing at any time (this only applies if consent is the only lawful basis the school has for processing)
- request that the school rectify, restrict or cease processing of their personal data in certain circumstances
- request the school erase records containing their personal data
- object to any decisions taken which were based solely on automated decision making or profiling (i.e. decisions not made by humans)
- be notified of any data breach which may affect them
- complaint to the ICO about how the school processes their data

All staff must notify the DPO if they receive a request from an individual relating to any of the above rights.

8. Parental Requests to see Educational Records

8.1. Entitled Persons (parents, carers or anybody with formal Parental Responsibility) have a separate legal right to access their child's educational records. This relates to the pupil file and will contain most of the information the school holds about a pupil. The school must provide parental access to educational records within 15 days of receipt of a written request.

9. Information Sharing

9.1. The school is committed to sharing information where it is appropriate to do so, whilst ensuring that this is done in a fair and transparent way which is in line with the rights and expectations of data subjects. In order to ensure a consistent approach the school will follow **The Information Sharing Procedure**.

9.2. The school will ensure that any routine information sharing for statutory purposes, or purposes otherwise identified as a substantial public interest task, will be described in the school's Privacy Notice.

9.3. The school will ensure that any third party data processors we engage to provide the services described in the privacy notice sign an agreement setting out;

- how and why they are allowed to process personal data shared by the school;
- how it will be securely shared; and
- how long the data processor can retain records of the personal data

9.4. The school will ensure that personal data is not used for any unsolicited direct marketing.

10. Security

The school will protect the personal data it holds from unauthorised or unlawful access, alteration, processing or disclosure and against any accidental or unlawful loss, destruction or damage. In particular:

- The school will ensure that personal data is stored securely and using modern software that is kept-up-to-date with regard to electronic records.

- Encryption software will be used to protect all portable devices and media such as laptops or USB sticks.
- Paper records and portable devices will be kept in a locked room or cupboard when not in use.
- Access to personal data shall be limited to school personnel who require such access to carry out their roles and responsibilities in order for the school to function.
- Appropriate security measures shall be in place to avoid unauthorised access to or sharing of personal information by school personnel.
- Appropriate security measures shall be identified and documented in the Information Asset Register.
- When electronic records containing personal data are deleted this must be done safely such that the data is irrecoverable.
- When hard copy/paper records containing personal data are destroyed this must be done safely such the data is irrecoverable.
- Appropriate back-up and disaster recovery solutions shall be in place to avoid the unintentional loss of personal data.

11. Data Breaches

11.1. In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the school shall promptly assess the risk to the data subject's rights and freedoms and, if appropriate, report this breach to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

11.2. In the event the school identifies a high risk of any harm or distress to any data subject as a result of a data breach the school shall notify that data subject without undue delay.

11.3. The school shall develop robust breach detection, investigation and internal reporting procedures to facilitate decision making about whether or not the relevant authorities and affected individuals are notified. Some guidance for doing so is listed as **Appendix A**.

12. CCTV

12.1. The school will adhere to the ICO's CCTV Code of Practice for use of CCTV footage.

12.2. The school does not need to seek consent to use CCTV for the purposes of maintaining security and preventing/detecting crime.

12.3. The school will ensure that clear signs are placed in areas where CCTV is in operation explaining that CCTV is in use.

13. Photographs and Video

13.1. As part of our school activities, we may take photographs and records images of individuals within the school.

13.2. The school will seek affirmative written consent from parents/carers for photographs and videos of their child to be used in any communications, marketing or promotional materials. In seeking such consent the school will explain clearly how and why the photographs/videos will be used.

13.3. Consent can be refused or withdrawn at any time. If consent is withdrawn the school will delete the photo or video and ensure it is not distributed any further.

13.3. Parents/carers are allowed to take photographs and videos at school events provided they are for their own personal use.

14. Training

14.1. All staff and governors will receive data protection training as part of their induction process.

14.2. Data protection will form part of continuing professional development to reflect any changes to information legislation or statutory guidance.

END OF POLICY

Appendix A: Personal data breach procedure

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

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

So, a data breach has occurred if personal data has been lost, stolen, destroyed (accidentally or in error), altered (accidentally or in error), disclosed accidentally or in circumstances where it should not have been or otherwise made available to unauthorised people.

Step 1: On finding or having caused a data breach, staff members or third party data processors must notify the Data Protection Officer immediately.

Step 2: The DPO must notify the headteacher and the Chair of Governors immediately when notified of a breach.

Step 3: The DPO will take all reasonable steps to contain the breach and minimise its effects as far as possible, requesting action from school staff members and any third party data processors that may be required.

- Can the data be retrieved or safely deleted/destroyed by any unintended recipient(s)?
- Are we certain we have identified all the data that was lost/mistakenly disclosed or altered etc?

Step 4: At the earliest possible time, the DPO will assess the potential consequences of the breach. The DPO should consider;

- How it could affect the data subject(s) involved?
- How serious will these effects be for the data subjects?
- How likely is it that the data subjects could be affected in this way(s)?

Step 5: The DPO must decide whether or not the breach must be reported to the ICO. Breaches must be considered on a case-by-case basis, however, a breach must be reported to the ICO if it is likely to result in any physical, material or non-material damage such as;

- loss of control over their personal data
- limitation of their rights
- discrimination
- identity theft or fraud
- financial loss
- unauthorised reversal of pseudonymisation
- damage to reputation
- or any other significant economic or social disadvantage to the individual(s) concerned

If the breach is likely to affect anybody in any of the ways described above, and cannot be successfully contained or rectified, it must be reported to the ICO.

Step 6: The DPO will document the decision taken as to whether or not the ICO are notified of

the breach. The school should keep a record of this decision in case it is challenged at a later date by any of the individuals involved or by the ICO. The school should keep a record of breaches whether or not they are reported to the ICO. This record should include;

- A description of the breach and how it occurred
- Details of the data involved
- A description of the potential consequences of the breach
- Details of how likely it is any individuals could be affected
- A description of measures taken to contain or rectify the breach
- Actions taken to avoid any repeat of errors that lead to the breach

Step 8: In cases where the breach must be reported to the ICO, the DPO (or another member of staff if they are not available) must do so within 72 hours of becoming aware of the breach. Such breaches are reported via the relevant page on the ICO's website.

Step 9: The DPO must decide whether or not the individual's affected by the breach must be notified. Again, the potential risks to any affected individuals (described in Step 5), the severity of any affects and the likelihood of them being affected must guide this decision making process. If there is a high risk the DPO will notify, in writing, all potentially affected individuals. This notification will include;

- Contact details for the DPO
- A description of how the breach occurred and the data involved
- A description of the measures taken to contain or rectify the breach
- Any advice it is possible to provide in terms of how the individuals could be affected

Step 10: The DPO must ensure records of breaches and decisions taken relating to them are stored and accessible in the event of any subsequent investigation by the school or the ICO.