Bevendean Primary School

Data Protection Policy

This policy was adopted in **May 2016**

This Policy is due for review in **June 2019**

Data Protection Officer: James England: dpo@dataprotection.education

Contents

1. Introduction

On the 25th May 2018 the current Data Protection Act will be replaced with the General Data Protection Regulation (GDPR).

This policy is designed to set out the ways in which personal data of staff, governors, students, parents or carers and other relevant individuals is processed fairly and lawfully.
Bevendean Primary School collects and uses personal information about our staff, governors, parents or carers, students and other individuals that may come into contact with the school. We collect this information so that we can fulfil our educational and other associated obligations and functions. In addition to this, there may also be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Bevendean Primary School is defined as a data controller and must comply with the data protection principles in its processing of personal data. This also includes the way in which data is collected, stored, used, disclosed and destroyed. We are also obliged to demonstrate compliance with the GDPR. Our failure to comply with the principles could expose the school and its staff to criminal and civil claims and possibly a financial penalty.

To view the school's purpose for holding and processing data, search for our school at https://ico.org.uk/esdwebpages/search and enter our name or ICO registration number.
Our school registration number is 0303 123 1113. This registration is renewed on an annual basis and updated whenever necessary.

2. Aims

Bevendean Primary School aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions as outlined in the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

That all those involved with the school community will have their data protection rights safeguarded.

Any staff member that is involved in the collection, processing or disclosure of personal data will be aware of their duties and responsibilities under this policy.

3. Scope

This policy will apply to the following:
The personal data of all staff, governors, parents or carers, students, trainee teachers or any individual carrying out duties on behalf of the school.

All personal data, whether it is in paper or electronic format.

4. Definitions

Personal Data – Any data relating to a living person who is directly or indirectly identifiable
Special Category (Sensitive) Data – Data relating to a person's race, ethnic origin, politics, religion, trade union membership, genetics, biometric, health, sex life or sexual orientation

Data Controller – The organisation which either individually or jointly decides the purposes and methods of data processing.
Data Processor – An organisation which processes data on behalf of the data controller
Processing – Just about anything which can be done with personal data

5. Principles

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- 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;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods in so far 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.
- 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.

GDPR also requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

Our school has processes in place for dealing with the exercise of the following rights by staff, students, governors, parents and members of the public in respect of their personal data.

6. The Right to be Informed

- Individuals will be supplied with a privacy notice that outlines what data is being held, the purpose of processing, its retention period and who it will be shared with. The privacy notice will be written in clear, plain language which is concise, transparent and easily accessible. There will be no charge made for this information.
- Privacy information will be supplied to you at the time we collect your personal data.

- We will regularly review, and where necessary, update our privacy information. We will bring any new uses of your personal data to your attention before we start processing it.

7. Right of Access

Under the GDPR, individuals will have the right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data via the submission of a Subject Access Request (SAR)

Subject Access Requests (SAR)

- Requests should be submitted in writing, either on paper or in electronic form to the DPO. Please include the name of the individual, an email address, contact phone number and details of the information being requested.
- Before any information is supplied, the school will verify the identity of the requesting individual using any reasonable means.
- We will provide a copy of the information **free of charge**. However, we will charge a 'reasonable fee' when a request is manifestly unfounded or excessive or if you ask us to supply further copies of the same information. All fees will be based on the administrative costs of providing the information.
- If the request is made electronically, we may provide the information in a commonly used electronic format.
- All Information will be provided without delay and at the latest within one month of receipt. We will promptly contact you to confirm receipt of your request.
- If a SAR is made for information containing, in whole or in part, a pupil's 'educational record', a response must be provided within 15 school days (in England, Wales and Northern Ireland this right of access is only relevant to maintained schools – not independent schools, English academies or free schools).
- We will extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.
- Where requests are manifestly unfounded or excessive, we hold the right to refuse to respond to the request. You will be informed of the reason why and we will inform you of your right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.
- Where we process a large quantity of information about an individual, the GDPR permits the school to ask the individual to specify the information the request relates to.

8. The Right to Rectification

- Individuals are entitled to have inaccurate personal data rectified, or completed if it is incomplete.

- Any requests for data rectification will be responded to within one month. This will be extended by two months if the request is complex. If this is the case the school will let the individual know without undue delay and within one month of receiving the request and explain why the extension is necessary.

- Where no action is being taken in response to a rectification request, we will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to their ability to seek to enforce this right through a judicial remedy.

- If the school disclosed the personal data to other third parties, we will contact each party and inform them of the rectification or completion of the personal data.

9. The Right to Erasure

The right to erasure is not absolute and only applies in certain circumstances.

- An individual has the right to erasure of their data if there is no longer a reason for its processing.

Individuals have the right to have their personal data erased if:

- The personal data is no longer necessary for the purpose which the school originally collected or processed it for.

- If the basis for processing was consent and this has now been withdrawn.

- The individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing.

- If the school has processed the personal data unlawfully.

- If the school has to do it to comply with a legal obligation

- If the school has processed the personal data to offer information society services to a child.

The right to erasure does not apply and can be refused if processing is necessary for one of the following reasons:

- To exercise the right of freedom of expression and information.

- To comply with a legal obligation.

- For the performance of a task carried out in the public interest or in the exercise of official authority.

- For archiving purposes in the public interest, scientific research historical research or statistical purposes.

- The exercise or defence of legal claims.

- If the processing is necessary for public health purposes in the public interest. This is for special category (sensitive) data only.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of their data, regardless of age at the time of the request.

The GDPR specifies two circumstances where the school will tell other organisations about the erasure of personal data:

- If the personal data has been disclosed to other third parties, unless this proves impossible or involves disproportionate effort.

- Where personal data has been made public in an online environment (such as social media, a forum or a blog) reasonable steps will be taken to inform other third parties who are processing the personal data to erase links to, copies or replication of that data.

10. The Right to Restrict Processing

- Individuals have the right to request that the school restricts or suppresses the processing of their personal data.

- When processing is restricted, the school is permitted to store the personal data, but not to further process it.

The school will restrict the processing of personal data in the following circumstances:

- If the individual contests the accuracy of their personal data, until the school can verify the accuracy of the data.

- If the data has been unlawfully processed and the individual opposes erasure and requests restriction instead.

- If the school no longer needs the personal data but the individual needs the school to keep it in order to establish, exercise or defend a legal claim.
- The individual has objected to the school processing their data and the school is considering whether our legitimate grounds override those of the individual.

The GDPR specifies where the school will tell other organisations about the erasure of personal data:

- If the personal data has been disclosed to other third parties, unless this proves impossible or involves disproportionate effort.

Once the school has made a decision on the accuracy of the data, or whether our legitimate grounds override those of the individual, we may decide to lift the restriction.

If we do this, we will inform the individual **before** we lift the restriction.

11. The Right to Data Portability

- Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

- It allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- To personal data that an individual has provided to a controller.
- Where the processing is based on the individual's consent or for the performance of a contract.
- When processing is carried out by automated means.

The school will provide the personal data in a structured, commonly used and machine readable form.

The school will provide the information free of charge.

If the individual requests it, the school may be required to transmit the data directly to another organisation if this is technically feasible. However, the school is not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any portability requests within one month.

This can be extended by two months where the request is complex or the school receives a number of requests. The school will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where the school is not taking action in response to a request, the school will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

12. The Right to Object

The school will clearly inform data subjects of their right to object at the first point of communication and within our privacy notices. This information will be presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on the performance of a task in the public interest.
- Direct marketing.
- Processing for purposes of scientific/historical research and statistics.

When personal data is processed for the performance of a legal task:

- Individuals must have an objection on "grounds relating to his or her particular situation".
- Bevendean Primary School will stop processing the personal data unless the processing is for the establishment, exercise or defence of legal claims or we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

When personal data is processed for direct marketing purposes:

- Bevendean Primary School will stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds for the school to refuse.

When personal data is processed for research purposes:

- Individuals must have an objection on "grounds relating to his or her particular situation".
- If the school is conducting research where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing.
- The school will provide you with a method to object online if any of the processing activities outlined above are carried out online.

13. Not to be Subject to Automated Decision Making or Profiling

The GDPR states that,

"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

For something to be solely automated there must be no human involvement in the decision-making process.

Bevendean Primary School will ensure that you can:

- Obtain human intervention
- Express your point of view
- Obtain an explanation of the decision and challenge it

If we are automatically processing personal data for profiling purposes, we will ensure that appropriate safeguards are put in place. This will include:

- Being as clear and transparent about the process as possible.
- Providing you with meaningful information about the logic involved in the decision-making process, as well as the significance and potential consequences to the individual.
- Using appropriate mathematical or statistical procedures.
- Minimising the risk of errors and allowing you to correct any inaccuracies by putting appropriate technical and organisational measures in place.
- Secure personal data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

The school will not usually use children's personal data to make solely automated decisions about them if these will have a legal or similarly significant effect upon them unless:

- We have the data subject's explicit consent.
- There are reasons of substantial public interest based on Union or Member State law.

14. Privacy by Design

Under the GDPR, the school has an obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities.

Data Protection Impact Assessments (DPIA)

Bevendean Primary School will use a DPIA to systematically analyse our processing and help us identify and minimise data protection risks by:

- Describing the processing and the purposes.
- Assess necessity and proportionality.
- Identify and assess risks to individuals.
- Identify any measures to mitigate those risks and protect our data.

A DPIA does not have to eradicate the risk, but should help to minimise risks and consider whether or not they are justified.

We will conduct a DPIA for processing that is likely to be high risk.

Our school will ensure that all DPIAs include the following information:

- A description and purpose of the processing.
- An assessment of necessity and proportionality.
- Identify and assess any risks to individuals.
- Identify any measures to mitigate those risks and protect the data.

Where a DPIA indicates high risk data processing, the school may consult the ICO to seek its opinion as to whether the processing of the data is GDPR compliant.

15. Data Breaches

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.

The Headteacher and School Business Manager will ensure that all school staff are aware of and understand what a data breach is. This will be part of any data protection training.

When a personal data breach has occurred, the school will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO.

The school will report any notifiable breaches to the ICO without undue delay, but not later than 72 hours after becoming aware of it.

The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis.

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the school will inform those concerned directly and without undue delay.

The school ensures we have robust breach detection, investigation and internal reporting procedures in place. This facilitates our decision-making about whether or not we need to notify the ICO and the affected individuals.

When reporting a breach to the ICO we will include the following information in our report:

- The nature of the personal data breach including, where possible the categories and approximate number of individuals and records concerned.
- The name and contact details of the data protection officer (DPO).
- A description of the likely consequences of the personal data breach.

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Failure to notify a breach when required to do so can result in a fine.

16. Data Security

It is the responsibility of all staff to ensure that the personal data that they process is stored securely and not disclosed to unauthorised third parties.
Access to personal data should only be granted to those individuals who need access for the purposes of their duties.
It will be the responsibility of the School Business Manager to ensure continuity and recovery measures are in place for the security of protected data.
Electronic devices used to store personal data will be protected with a password/passcode to protect against theft or unauthorised access. Where it is technically possible, the school may also insist on the remote erasure of data from electronic devices such as phones or tablets. This includes devices owned by staff if they are using them to access personal data processed by the school.
If staff or governors are using their own personal devices to access personal data owned by the school, then permission must be sought from Headteacher.
If staff are working from home, they must have particular regard to ensure compliance with this policy and the school 'Acceptable Use ICT' policy.
Data will be destroyed securely in accordance with the Information and Records Management Society Retention Guidelines for Schools (IMRS Toolkit)
A Data Protection Impact Assessment (DPIA) will be carried out where there are new types of personal data processing that may result in a high risk to the rights and freedoms of the individual.
All staff will be aware of and follow the data breach security management process.
Please see Appendix A for a list of staff Do's and Don'ts that relate to data security.

17. Sharing Personal Data

Personal data will only be shared with third parties where we deem it to be fair and lawful to do so.
If a third party is processing data on behalf of the school, we will ensure that there is a written agreement outlining the manner in which the data will be processed in accordance with the principles of the GDPR.

18. Ensuring Compliance

There will be training and guidance available to all staff.
New staff will receive data protection training as part of their induction and will be required to sign any relevant acceptable use policies.
The school will provide a Privacy notice to its workforce and parents/carers. This policy will contain the following information:

- The legal basis and purpose for data processing.
- The retention period and who the data is shared with.
- The right to request any rectifications, erasure, consent to withdraw, to complain, data portability (if applicable) and the right to know about automated decision processes.

19. Photographs

Please see the school's photography policy.

20. Monitoring

The school's DPO is responsible for the monitoring and review of this policy.
This policy will be reviewed every 2 years. The school may consider reviewing this policy within the first year of implementation.

21. Links with Other Policies

- eSafety and Acceptable Use Policy (Online Safety Policy)
- Images of Children Policy
- Child Protection and Safeguarding Procedures
- Social Networking Policy
- Staff Handbook
- Code of Conduct Policy

June 2018:

Our Data Protection Officer (DPO) is James England dpo@dataprotection.education

Appendix A

Staff Must:

- Ensure that confidential paper records are kept in locked filing cabinets or cupboards.
- Ensure that confidential paper records are not left unattended or in clear sight anywhere in the school that has general access.

- Ensure you have permission from the school/your line manager (Headteacher) before you remove any personal data from the building or take it home.
- Ensure that any electronic personal data is stored on an encrypted computing device or encrypted USB device when being removed from the school. * from September 2017, Bevendean Primary School started using OneDrive. All school data should be accessed via OneDrive. Staff must seek permission and inform the Headteacher if they transport information using an encrypted USB.
- Ensure that any personal data that has been taken home is locked away when being stored.
- Ensure that all paper based information that is taken of the premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.
- Do ensure that when transporting paper documentation in your car, that it is placed in the boot (locked) during transit.
- Do return the paper based information or portable computer devices to the Headteacher immediately.
- Ensure that paper based, personal data and/or laptops are kept close by and stored securely when taken offsite. Do not leave them unattended. Care should be taken in public places e.g. if reading personal data on a train or bus.
- When returning paper based personal data back to school, dispose of it or store it securely.

- Encrypt any email that contains personal data including attachments.
- Use the BCC option when emailing a large number of recipients or sending a circular email to parents.
- Ensure that all email and postal addresses are checked to ensure the safe dispatch of information. [If you are sending personal data by post, mark the envelope 'Private – Contents for Addressee only' and send the item either Recorded Delivery so that proof of postage can be gained.]

- Ensure that only the required information is posted to the recipient.
- Where possible use pseudonyms and anonymise personal data.
- Do ensure that access to SIMS is restricted to appropriate staff only, that leavers are removed in a timely manner and that generic user names such as 'Sysman' are disabled.

Staff Must Not:

- Take any personal data to a place of entertainment or public place such as a pub or cinema, unless it is required as part of an official school visit.
- Copy other parties unnecessarily into e-mail correspondence. Unless it is required, do not use the 'Reply All' option when responding to emails.
- E-mail documents containing personal data to their personal e-mail accounts/personal computing devices.
- Leave their computers unlocked or share their passwords with any other individual. If staff feel their password has been compromised a new one should be requested.
- Store work related personal data/documents on your own home computers.
- Leave any documents containing personal data unclaimed in or on any printer or fax machine.
- Print off documents containing personal data unless absolutely necessary.
- Leave personal data out on your desk overnight or if you are away from your desk. Lock the door if this is possible.
- Leave personal data in a vehicle overnight.
- Discuss issues regarding personal data at social events or in a public place.
- Dispose of personal information/data in non-confidential bins.
- Use unencrypted USB storage devices or laptops.