Dame Ellen Pinsent
GDPR (Data Protection) Policy

Last Review: 7th June 2019
Ratified by Governors FGB
To be Reviewed May 2020
Statement of intent

Dame Ellen Pinsent School is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children’s services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the school complies with the following core principles of the GDPR.

Organisational methods for keeping data secure are imperative, and Dame Ellen Pinsent School believes that it is good practice to keep clear practical policies, backed up by written procedures.

This policy complies with the requirements set out in the GDPR, which came into effect on 25 May 2018. The government have confirmed that the UK’s decision to leave the EU will not affect the commencement of the GDPR.
1. Legal framework

1.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation (GDPR)
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

1.2. This policy will also have regard to the following guidance:

- Information Commissioner’s Office (2017) ‘Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now’

1.3. This policy will be implemented in conjunction with the following other school policies:

- Photography and Videos at School Policy
- E-safety Policy
- Freedom of Information Policy
- CCTV Policy

2. Applicable data

2.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

2.2. **Sensitive personal data** is referred to in the GDPR as ‘special categories of personal data’, which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.
3. Principles

3.1. In accordance with the requirements outlined in the GDPR, personal data will 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 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.
- 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.

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

4. Accountability

4.1. Dame Ellen Pinsent School’ will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

4.2. The school will provide comprehensive, clear and transparent privacy policies.

4.3. Records of activities relating to higher risk processing will be maintained, such as the processing of special categories data or that in relation to criminal convictions and offences.

4.4. Internal records of processing activities will include the following:

- Name and details of the organisation
4.5. The school will implement measures that meet the principles of data protection by design and data protection by default, such as:

- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.

4.6. Data protection impact assessments will be used, where appropriate.

5. **Data protection officer (DPO)**

5.1. A DPO will be appointed in order to:

- Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the school’s compliance with the GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

5.2. An existing employee might be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests. However, the school have the right to employ DPO externally if required.

5.3. The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.

5.4. The DPO will report to the highest level of management at the school, which is the Executive Head teacher.

5.5. The DPO will operate independently and will not be dismissed or penalised for performing their task.

5.6. Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6. **Lawful processing**
6.1. The legal basis for processing data will be identified and documented prior to data being processed.

6.2. Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the school in the performance of its tasks.)

6.3. Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
- Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
  - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring
high standards of healthcare and of medicinal products or medical devices.

— Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

7. Consent

7.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

7.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual’s wishes.

7.3. Where consent is given, a record will be kept documenting how and when consent was given.

7.4. The school ensures that consent mechanisms meet the standards of the GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

7.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

7.6. Consent can be withdrawn by the individual at any time.

7.7. Where a child is under the age of 16 [or younger if the law provides it (up to the age of 13)], the consent of parents will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

7.8. See appendix 1

8. The right to be informed

8.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

8.2. If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand. (see appendix 2)

8.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller’s representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
• Details of transfers to third countries and the safeguards in place.
• The retention period of criteria used to determine the retention period.
• The existence of the data subject’s rights, including the right to:
  — Withdraw consent at any time.
  — Lodge a complaint with a supervisory authority.
• The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

8.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

8.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the school holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

8.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained.

8.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:
• Within one month of having obtained the data.
• If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
• If the data are used to communicate with the individual, at the latest, when the first communication takes place.

9. The right of access

9.1. Individuals have the right to obtain confirmation that their data is being processed.

9.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

9.3. The school will verify the identity of the person making the request before any information is supplied.

9.4. A copy of the information will be supplied to the individual free of charge; however, the school may impose a ‘reasonable fee’ to comply with requests for further copies of the same information.

9.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

9.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

9.7. All fees will be based on the administrative cost of providing the information.
9.8. All requests will be responded to without delay and at the latest, within one month of receipt.

9.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension, and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

9.10. Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

9.11. In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

10. The right to rectification

10.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

10.2. Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible.

10.3. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

10.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

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

11. The right to erasure

11.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

11.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child
11.3. The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

11.4. 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 the data, regardless of age at the time of the request.

11.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

11.6. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

12. **The right to restrict processing**

12.1. Individuals have the right to block or suppress the school’s processing of personal data.

12.2. In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

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

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim
12.4. If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.5. The school will inform individuals when a restriction on processing has been lifted.

13. **The right to data portability**

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

13.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

13.3. The right to data portability only applies in the following cases:

- 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

13.4. Personal data will be provided in a structured, commonly used and machine-readable form.

13.5. The school will provide the information free of charge.

13.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

13.7. The school is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

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

13.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

13.11. Where no action is being taken in response to a request, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

14. **The right to object**

14.1. The school will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and
explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

14.2. Individuals have the right to object to the following:

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

14.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

14.4. Where personal data is processed for direct marketing purposes:

- The school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

14.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- 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 of the data.

14.6. Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.

15. **Automated decision making and profiling**

15.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

15.2. The school will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

15.3. When automatically processing personal data for profiling purposes, the school will ensure that the appropriate safeguards are in place, including:
• Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.

• Using appropriate mathematical or statistical procedures.

• Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

• Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

15.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

• The school has the explicit consent of the individual.

• The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

16. Privacy by design and privacy impact assessments

16.1. The school will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

16.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the school’s data protection obligations and meeting individuals’ expectations of privacy.

16.3. DPIAs will allow the school to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the school’s reputation which might otherwise occur.

16.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

16.5. A DPIA will be used for more than one project, where necessary.

16.6. High risk processing includes, but is not limited to, the following:

• Systematic and extensive processing activities, such as profiling

• Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences

• The use of CCTV.

16.7. The school will ensure that all DPIAs include the following information:

• A description of the processing operations and the purposes

• An assessment of the necessity and proportionality of the processing in relation to the purpose
16.8. Where a DPIA indicates high risk data processing, the school will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

17. **Data breaches**

17.1. The term ‘personal data breach’ refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

17.2. The Head teacher, with delegated responsibility will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

17.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

17.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the school becoming aware of it.

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

17.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the school will notify those concerned directly.

17.7. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

17.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

17.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

17.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects
17.11. Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

18. **Data security**

18.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

18.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

18.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

18.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.

18.5. Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.

18.6. All electronic devices are password-protected to protect the information on the device in case of theft.

18.7. Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft.

18.8. All necessary members of staff are provided with their own secure login and password, and passwords are changed as and when needed.

18.9. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

18.10. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

18.11. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

18.12. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.

18.13. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

18.14. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the school containing sensitive information are supervised at all times.
18.15. The physical security of the school’s buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

18.16. Dame Ellen Pinsent School’ takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

18.17. The DPO continuity and recovery measures are in place to ensure the security of protected data.

19. **Publication of information**

19.1. Dame Ellen Pinsent School’ publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Financial information

19.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

19.3. Dame Ellen Pinsent School’ will not publish any personal information, including photos, on its website without the permission of the affected individual.

19.4. When uploading information to the school website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

20. **CCTV and photography**

20.1. The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. Currently Dame Ellen Pinsent do not operate CCTV should we change this decision the following will apply.

20.2. The school notifies all pupils, staff and visitors of the purpose of CCTV via notice boards, letters and email.

20.3. A camera is only placed where they do not intrude on anyone’s privacy and are necessary to fulfil their purpose.

20.4. The CCTV is for live monitoring purpose only and does not record any footage.

20.5. The school will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them. Parental consent forms are issued when a child starts school.

20.6. If the school wishes to use images/video footage of pupils in a specific publication, such as recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.
20.7. Precautions, as outlined in the ‘Photography and Videos consent form’, are taken when publishing photographs of pupils, in print, video or on the school website.

20.8. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, must only contain images of their own children and if not cannot be published on social media. Personal images of parents own children are exempt from the GDPR.

21. **Data retention**

   21.1. Data will not be kept for longer than is necessary.

   21.2. Unrequired data will be deleted/destroyed as soon as practicable.

   21.3. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.

   21.4. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained by a reputable service.

22. **DBS data**

   22.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

   22.2. Data provided by the DBS will never be duplicated.

   22.3. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

23. **Policy review**

   23.1. This policy is reviewed annually by the Data Protection Officer and the Executive Head teacher.

   The next scheduled review date for this policy is May 2020.
Appendix 1

Parental consent form Images and videos
This form explains the reasons why and how Dame Ellen Pinsent may use images and videos of your child. Please read the form thoroughly and outline your agreement as appropriate.

<table>
<thead>
<tr>
<th>Name of parent/carer:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Email of parent/carer:</td>
<td></td>
</tr>
<tr>
<td>Name of pupil:</td>
<td></td>
</tr>
<tr>
<td>Date consent form completed:</td>
<td></td>
</tr>
<tr>
<td>Current Class:</td>
<td></td>
</tr>
</tbody>
</table>

Why do we need your consent?
Dame Ellen Pinsent school requests the consent of parents/carers to use images and videos of their child/children for a variety of different purposes. Without your consent, the school will not use images and videos of your child. Similarly, if there are only certain conditions under which you would like images and videos of your child to be used, the school will abide by the conditions you outline in this form.

Why do you we use images and videos of your child?
Dame Ellen Pinsent uses images and videos of pupils as part of school displays & media posts to celebrate school life and pupils’ achievements; to promote the school on social media and on the school website; and for other publicity purposes in printed publications, such as newspapers, news broadcasts or publications by visiting companies who have provided an organised event or activity that children have participated in, for example CBeebies, Birmingham Climbing Wall, CBSO, The Animal Man etc.

Dame Ellen Pinsent may take images or videos of individual pupils and groups of pupils to use on social media, the school website, twitter, in school prospectuses and other printed publications, such as a newsletter. Where the use of images/videos of individual pupils occurs, the name of the pupil will not be disclosed. Where an individual pupil is named in a written publication, a photograph of the pupil will not be used to accompany the text unless express permission has been requested prior to use, for example, a pupil has won an award and their parent would like their name to be published alongside their image, separate consent will be obtained prior to this.

Who else uses images and videos of your child? 3rd Parties.
It is common that the school is visited by local media and press and service providers for organised activities, who may take images or videos of school events, such as sports days, pantomime, Forest School events and Educational visits etc. Pupils will appear in these images and videos, and these may be published in local or national newspapers, or on approved websites of the service providers (3rd Parties).
The following may use images and videos of your children, the following are examples but are not limited to:

- Local Newspapers
- Birmingham City Council
- Local News
- Educational visit locations
Linked schools and associated organised school activities
Where any organisations other than those above intend to use images or videos of your child, additional consent will be sought before any image or video is used.

What are the conditions of use?
- This consent form is valid for the duration that your child attends the school.
- It is the responsibility of parents to inform the school, in writing, if consent needs to be withdrawn or amended.
- The school will not use the personal details or full names of any pupil in an image or video, on our website, in our school prospectuses or any other printed publications.
- The school will not include personal emails or postal addresses, telephone or fax numbers on images or videos on our website, in our school prospectuses or any other printed publications.
- The school may use pictures of pupils and teachers that have been drawn by pupils.
- The school may use work created by pupils.
- The school may use group or class images or videos with general labels, e.g. ‘sports day’.
- The school will only use images and videos of pupils who are suitably dressed, i.e. it would not be suitable to display an image of a pupil in swimwear.
- The school will take class images of your child which are available to purchase annually.

Providing your consent
Please read the following conditions thoroughly and provide your consent as appropriate by ticking either ‘Yes’ or ‘No’ for each criteria.

The school will only publish images and videos of your child for the conditions that you provide consent for. Please be aware that photographs are used in ALL Childrens work journals and permission is not required for such images as no personal data is detailed in these workbooks and they are not for use in the public domain.

<table>
<thead>
<tr>
<th>I provide consent for Dame Ellen Pinsent School to:</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use images/videos of my child/children for school use including displays, the school website social media including the school twitter account and any 3rd party events organised by the school and could include but is not exhaustive to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Twitter</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Blog sites</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Linked organised school activity providers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PLEASE NOTE: This does not permit other parents to post images/videos on their personal social media accounts unless their child is the only child in the video or photograph</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using images/videos of my child in marketing material, e.g. the school brochure and prospectus and 3rd party media.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sharing my child’s data with a school-appointed external photography company for official school images. This includes the following:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Roll number</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Refreshing your consent
This form is valid for the duration of your child’s time at Dame Ellen Pinsent. Parents will be reminded periodically about their right for withdrawal. Consent will also be refreshed where any changes to circumstances occur – this can include, but is not limited to, the following:

- New requirements for consent, e.g. an additional social media account will be used to share pupil images and videos
- Changes to a pupil’s circumstances, e.g. safeguarding requirements mean a pupil’s image cannot be used
- Changes to parental consent, e.g. amending the provisions for which consent has been provided for

Where you would like to amend the provisions for which consent has been provided, you must submit your request in writing, addressed to the Data Protection Officer (DPO). A new form will be supplied to you to amend your consent accordingly and provide a signature.

Withdrawing your consent
Parents have the right to withdraw their consent at any time. Withdrawing your consent will not affect the legality of processing images or videos that were shared prior to withdrawal; however, the school will make every effort to remove images of the pupil where possible, e.g. images of the pupil on the school’s website will be removed. If you would like to withdraw your consent, you must submit your request in writing to the DPO.

Declaration
I, ________________________________ (name of parent/carer),

Parent/carer of _________________________ Class___________

understand:

- Why my consent is required.
- The reasons why Dame Ellen Pinsent uses images and videos of my child.
- Other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my consent.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the DPO.

Signed…………………………………………………. (parent/carer)

Date…………………………..

If you have any questions regarding this form, please do not hesitate to contact the DPO at enquiry@dameellenpinsent.bham.sch.uk or 0121 675 2487.
Appendix 2

GDPR Privacy Notice (Pupils and their families)

Data Protection Officer (DPO)?
The Data protection officer is responsible for overseeing Dame Ellen Pinsent’s data protection strategy and its implementation to ensure compliance with GDPR requirements.

Who processes your information?
Dame Ellen Pinsent School is the data controller. This means the school determines the purposes for which any personal data relating to pupils and their families is to be processed.

Why do we collect and use your information?
The personal data of pupils and their families is collected and used for the following reasons:

- To support monitor & report pupil learning and pupil progress
- To provide appropriate pastoral care
- To safeguard the children
- To assess performance

In accordance with the regulation, to meet legal obligations and legitimate interests set out in the GDPR and UK law including those in relation to the following:

- Article 6 and Article 9 of the GDPR
- Education Act 1996
- Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013
- Working together to Safeguard Children 2015
- Keeping Children Safe in Education 2016
- Safeguarding Vulnerable Groups Act 2006

What data is collected?
The information that the school collects, holds and shares can include the following:

- Personal information – e.g. names, pupil numbers and addresses, ethnicity, language, nationality, country of birth. Medical information, SEND (EHCP), assessment and attendance, Free School meal eligibility, dietary information.
- Behavioural information – e.g. number of temporary exclusions

Whilst the majority of the personal data you provide to the school is mandatory, some is provided on a voluntary basis. When collecting data, the school will inform you whether you are required to provide this data or if your consent is needed. Where consent is required, the school will provide you with specific and explicit information with regards to the reasons the data is being collected and how the data will be used.

How long is your data stored for?
Personal data relating to pupils at Dame Ellen Pinsent School and their families is stored in accordance with the school’s GDPR Data Protection Policy (available on our website), data is stored for as long as is necessary to complete the task for which it was originally collected.

Will my information be shared?
Yes - All schools are required to share pupils’ data with the DfE on a statutory basis, this includes the following:
The National Pupil Database (NPD) is managed by the DfE and contains information about pupils in schools in England. Dame Ellen Pinsent School is required by law to provide information about our pupils to the DfE as part of statutory data collections, such as the school census; some of this information is then stored in the NPD. The DfE may share information about our pupils from the NDP with third parties who promote the education or wellbeing of children in England by:

- Conducting research or analysis.
- Producing statistics.
- Providing information, advice or guidance.

The DfE has robust processes in place to ensure the confidentiality of any data shared from the NDP is maintained. The school routinely shares pupils’ information with:

- Pupils’ secondary schools (compulsory)
- The Local Authority (compulsory)
- The NHS (compulsory)
- The Department for Education (compulsory)
- Travel Assist (compulsory)

The following are essential operational systems for our school to function and in some cases are managed by a third-party processor or hosted by cloud services:

- School Management Information System
- Text message/ email service
- ICT - Support and Remote Access
- Visitor Management Software
- School assessment system
- Behavioural monitoring system
- Child Protection Data base
- Cashless payment system

Where the school outsources data to a third-party, the same data protection standards that Dame Ellen Pinsent School comply with, are imposed on the processor. Data is only shared where the Law requires it. The information that we share with these parties includes the following:

- Child names, dates of birth, year group, addresses and parent/carers names and addresses.

**What are your rights?**

Parents and pupils have the following rights in relation to the processing of their personal data.

You have the right to:

- Be informed about how Dame Ellen Pinsent School uses your personal data.
- Request access to the personal data that Dame Ellen Pinsent School hold.
- Request that your personal data is amended if it is inaccurate or incomplete.
- Request that your personal data is erased where there is no compelling reason for its continued processing.
- Request that the processing of your data is restricted.
- Object to your personal data being processed (in some circumstances).

Where the processing of your data is based on your consent, you have the right to withdraw this consent at any time.
If you have a concern about the way Dame Ellen Pinsent School and/or the Department for Education (DfE) is collecting or using your personal data, you can raise a concern with the Information Commissioner’s Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

You can also contact our Data Protection Officer at enquiry@dameellenpinsent.bham.sch.uk marking your email For the Attention of the DPO

---

**GDPR Parent/Carer Declaration**

We require consent for all children in school, we can no longer assume that no response means that you give consent. Thank you for your support.

I, ___________________________ Parent/Carer of _________________________________

Understand that Dame Ellen Pinsent School has a legal and legitimate interest to collect and process my child and family’s personal data to meet statutory requirements as detailed in this privacy statement and I give my consent to this.

**Child Name(s):**

____________________________________________________________

**Your Name:**

____________________________________________________________

**Signature:**

____________________________________________________________

**Date:**

____________________________________________________________