Data Protection Policy

Version 2.0

peletrust.org.uk
The Crescent, Callerton Lane, Ponteland, NE20 9EG

Contents

1. Introduction

Pele Trust, and its schools, is required to keep and process personal information about its organisation, staff members and pupils in accordance with its legal obligations under the 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.

This policy is in place to ensure all Pele Trust staff, Board of Directors and Academy Committee members are aware of their responsibilities; and outlines how the Trust and/or its schools complies with the core principles of the GDPR.

This policy complies with the requirements set out in the GDPR, which came into effect in May 2018.

2. Legal framework

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

- The General Data Protection Regulation
- 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

This policy also has regard to the following guidance:

- ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)'

3. Applicable data

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 or UPN. 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.

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.

4. Principles

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.

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

5. Accountability

Pele Trust is the data Controller on behalf of its schools and will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the GDPR.

The Trust will provide comprehensive, clear and transparent privacy notices for staff, parents and carers and pupils.

Where required, the Trust and/or its schools will undertake a Data Protection Impact Assessment and ensure that records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.
- Use new technologies.

The Trust and/or its schools will maintain internal records of processing activities (a data map) which will include the following:

- Record name
- Source of data
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place

The Trust and/or its schools 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.

Data protection impact assessments will be used, where appropriate.

6. Data protection officer (DPO)

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.

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

The DPO will report to the highest level of management at the school, which is the headteacher, will operate independently and will not be dismissed or penalised for performing their task.

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

7. Lawful processing

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

In the school context the majority of personal information can and will be lawfully processed because 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.)

There are some instances where the provision of personal information is not compulsory. Where this is the case the consent of the data subject will be sought prior to processing personal identifiable information.

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.

Or where 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).

8. Consent

Where the Trust and/or its schools seek consent to process personal data it will seek a positive indication. It will not be inferred from silence, inactivity, nil response or pre-ticked boxes.

Consent will only be accepted where it is freely given, is specific to the purposes for which the information is intended, informed and an unambiguous indication of the individual's wishes.

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

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 re-obtained.

Consent can be withdrawn by the individual at any time.

Where a child is under the age of 16 (or younger if the law provides it i.e. 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.

9. The right to be informed

The Trust and/or its schools will publish privacy notices in regards to the processing of personal data and they will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

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.

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:
    - 1. Withdraw consent at any time.
    - 2. 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.

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.

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.

10. The right of access

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

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.

The Trust and/or its schools will verify the identity of the person making the request before any information is supplied.

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 that are manifestly unfounded, excessive or for further copies of the same information. All fees will be based on the administrative cost of providing the information.

When responding to a SAR information will usually be provided in a commonly used electronic format however the subject may request an alternative format.

ICO guidance says it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a subject access request for information held about a child, the school will consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we will usually respond directly to the child. We will allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child.

All requests will be responded to without delay and at the latest, within one month of receipt.

In the event of numerous or complex requests from a data subject the period of compliance may be extended by up to 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.

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.

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.

11. The right to rectification

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

Where the personal data in question has been disclosed to third parties, they will be informed of the rectification where possible.

Where appropriate, the individual will be informed about the third parties that the data has been disclosed to.

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

Where no action is being taken in response to a request for rectification, an explanation as to the reason for this will be offered to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

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

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

The Trust and/or its schools 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

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.

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.

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

13. The right to restrict processing

Individuals have the right to block or suppress the Trust and/or its schools processing of personal data.
In the event that processing is restricted, personal data may be stored, but not further processed, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Trust and/or its schools 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

If the personal data in question has been disclosed to third parties, they will be informed about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust and/or its schools will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

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

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.

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

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

The Trust and/or its schools will provide the information free of charge except as outlined above.

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

The Trust and/or its schools is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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.

The Trust and/or its schools will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the time frame 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.

Where no action is being taken in response to a request, the Trust and/or its schools 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.

15. The right to object

The Trust and/or its schools will outline an individual's right to object in the privacy notice.

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.

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.

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.

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.

Where the processing activity is outlined above, but is carried out online, the Trust and/or its schools will offer a method for individuals to object online.

16. Automated decision making and profiling

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.

The Trust and/or its schools 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.

It the event that the Trust and/or its schools should automatically process personal data for profiling purposes, they 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.

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

- There is explicit consent of the individual and/or their parents.
- The processing is necessary for reasons of substantial public interest on the basis of EU/UK law.

17. Privacy by design and privacy impact assessments

The Trust and/or its schools 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.

As stated above, Data Protection Impact Assessments (DPIAs) will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the identification and resolution of problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust and/or its schools reputation which might otherwise occur.

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.

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

- 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.

The Trust and/or its schools 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
- An outline of the risks to individuals
- The measures implemented in order to address risk

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.

18. Data breaches

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.

The Trust has a Data Breach procedure and the Headteacher will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their training.

As set out in the Data Breach policy where a breach is likely to result in a risk to the rights and freedoms of individuals, and in accordance with the requirements of GDPR, the ICO will be informed.

All notifiable breaches will be reported at the earliest opportunity but certainly within the required 72 hours of the school becoming aware of it.

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

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

19. Data security

Confidential paper records will be maintained securely and with restricted access. Historical student and staff records will be stored securely either on site of offsite. Confidential paper records will not be left unattended or in clear view anywhere with general access.

Where data is saved on removable storage or a portable device, the device will be encrypted and kept secure when not in use.

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

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

Where possible, the school enables electronic devices to allow the remote blocking or deletion of data in case of theft (e.g. through use of Lightspeed MDM).

Staff will not use their personal laptops or computers for school purposes.

Staff are provided with their own secure login and password, and password protocols require a change of password every 90 days.

Emails containing sensitive or confidential information are encrypted if there are unsecure servers between the sender and the recipient.

Circular emails to parents are sent via School Comms, Mail Chimp or (less so) by blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

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

Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- The recipient of the data is someone who has been outlined in a privacy notice.

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.

The physical security of the school's buildings and storage systems, and access to them, is reviewed on a regular basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.

Pele Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

The school SLT is responsible for continuity and recovery measures are in place to ensure the security of protected data.

20. Publication of information

Pele Trust and its schools will not publish any personal information, including photos, on its websites without the permission of the affected individual and/or their parents.

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.

21. CCTV and photography

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The Trust and/or its schools notifies all pupils, staff and visitors of the purpose for collecting CCTV images via clearly placed signage around site.

Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All CCTV footage will be kept for 30 days for security purposes; the school SLT is responsible for keeping the records secure and allowing access.

The schools will always indicate its intentions for taking photographs of pupils and will review permissions before publishing them.

Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR.

22. Data retention

Data will not be kept for longer than is necessary. The Trust retention policy sets out how long information will be retained.

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.

Paper documents will be securely disposed of and electronic memories scrubbed clean and/or securely destroyed once the data should no longer be retained.

23. DBS data

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

Data provided by the DBS will never be duplicated.

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.

Document Control

Version number	Date of last review
2.0	November 2024