# Data Protection & Privacy Policy

Created in: May 2023
Review date: May 2024
Approved by: MP TO COMPLETE
Signature: MP TO COMPLETE

UNITED WE ARE WORLD CLASS>

# Contents

## Rationale

We need student, parent and employee personal data to run our Trust and its schools successfully. We are trusted to look after this essential information. In order to operate effectively, we may also collect and use information relating to the people with whom we work, such as members of the public, contractors and suppliers. In addition, we may be required by law to collect and use information in order to comply with the requirements of central government.

**Legal Framework**

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

- the UK General Data Protection Regulation (UK UK GDPR);
- the Data Protection Act 2018 (DPA 2018);
- the Freedom of Information Act 2000;
- the Protection of Freedoms Act 2012 (when referring to our use of biometric data);
- the ICO's code of practice for the use of surveillance cameras and personal information; and
- our funding agreement and articles of association.

We are committed to ensuring that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the UK UK GDPR (the EU UK GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020) and the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

We are committed to making every effort to meet our obligations under the UK GDPR legislation and will regularly review policies and procedures to ensure that we are doing so.

We recognise that each and every employee has a responsibility to comply with the appropriate data protection laws. Our schools and employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature. It is the responsibility of all members of the Trust community to take care when handling, using or transferring personal data so that it cannot be accessed by anyone who does not:

- have permission to access that data; and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and/or the school concerned, can bring the school and the Trust into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office (ICO). Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance.

The UK GDPR lays down a set of rules for processing of personal data (both structured manual records and digital records). The UK GDPR:

- defines what is meant by 'personal data';
- confers rights on 'data subjects';
- places obligations on 'data controllers' and 'data processors';
- creates principles relating to the processing of personal data; and
- it provides for penalties for failure to comply with the above.

**Personal Data**

Under the UK GDPR, personal data is defined as: *"Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

**The Six Principles of the UK GDPR**

Under the UK GDPR, the data protection principles set out the main responsibilities for organisations. The UK 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 are 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 UK GDPR in order to safeguard the rights and freedoms of individuals; and
- 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.

## Responsibilities

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

The Board of Trustees have overall responsibility for our compliance with the UK GDPR and have appointed a Data Protection Officer (DPO) to ensure compliance.

The CEO and Heads are responsible for ensuring compliance with the UK GDPR and this policy within the day-to-day activities of the Trust and our schools. The Data Protection Officer (DPO) will have the support of our CEO and Heads in order to ensure that appropriate training is provided for all staff.

Staff need to be aware of their obligations relating to any personal data they process as part of their duties. Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to disciplinary action and potentially criminal prosecution. Everyone has the responsibility of handling personal and sensitive personal data in a safe and secure manner.

The Trust and its schools will hold the minimum personal data necessary to enable them to perform their function and will not hold data for longer than necessary for the purposes it was collected for. Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

**Data Controller**
As a Multi Academy Trust (MAT), the PACT is responsible for the activities of all the schools in the MAT, even though some functions may have been delegated to local Heads or Academy Committees. Ultimate responsibility lies with the MAT. Therefore, the PACT is the legal entity responsible for the processing of personal data by the academies within the MAT, and so the PACT is the data controller subject to data protection obligations.

As a data controller, the PACT pays the appropriate Data Protection Fee to the Information Commissioner's Office on an annual basis and also provides contact details for our Data Protection Officer. The ICO publishes a register of fee paying organisations which can be checked online by visiting: https://ico.org.uk/esdwebpages/search.

**Board of Trustees and Academy Committees**
The Board of Trustees and Academy Committees are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Trustee or Representative.

**Data Protection Officer (DPO)**
The UK GDPR makes it a requirement for public authorities to appoint a Data Protection Officer (DPO). The UK GDPR defines the minimum tasks of the DPO as follows:

- to inform and advise the organisation and its employees about their obligations to comply with the UK GDPR and other data protection laws;
- to monitor compliance with the UK GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits; and
- to be the first point of contact for supervisory authorities and for individuals whose data is processed.

The DPO will operate independently reporting to the CEO for the Trust and will not be dismissed or penalised for performing their task and duties. The Trust will ensure that sufficient resources are provided to the DPO to enable them to meet their obligations.

GDPR Sentry Limited have been appointed as our DPO. You can contact our DPO by emailing dpo@the-pact.co.uk.

**Accountability**
The Prince Albert Community Trust will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR. We will provide comprehensive, clear and transparent privacy policies. As an employer with over 250 employees, additional internal records of our processing activities will be maintained and kept up-to-date. Internal records of processing activities will include the following:

- name and details of the organisation;
- 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; and
- details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.

The Prince Albert Community Trust 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; and
- use of data protection impact assessments, where appropriate.

# Personal Data

The UK GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier (such as IP address).

The UK GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the UK GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

**Sensitive Personal Data**
The UK GDPR has extended the definition of 'sensitive personal data' which requires even more protection than 'personal data'. Sensitive personal data includes data relating to the following:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data;
- health;
- sex life; and
- sexual orientation.

The Trust, our schools and our employees must be careful when handling sensitive personal data, especially if it's necessary to share it with other organisations, to ensure it is adequately protected at all times.

# Lawful Processing

Under the UK GDPR, before any personal data is processed, the data controller has to identify what legal basis they are using to process the data and ensure that this is recorded. The UK GDPR sets out six legal bases that a data controller can consider and record before processing personal data:

- consent of the data subject (or their parent/carer when appropriate in the case of a student);
- processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract;
- processing is necessary for compliance with a legal obligation;

- processing is necessary to protect the vital interests of a data subject or another person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and
- necessary 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. Note that this condition is not available to processing carried out by public authorities in the performance of their tasks.

If processing sensitive personal data, the UK GDPR sets out further legal bases that a data controller must consider and record before processing takes place:

- explicit consent of the data subject (or their parent/carer when appropriate in the case of a student);
- processing is necessary for carrying out obligations under employment, social security or social protection law, or a collective agreement;
- processing is necessary to protect the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent;
- 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 the establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity;
- processing is necessary for 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;
- processing is necessary for 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;
- processing is necessary for 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; and
- processing is necessary for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes.

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- the individual (or their parent/carer when appropriate in the case of a student) has given consent;
- the data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent;
- the data has already been made manifestly public by the individual;
- the data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- the data needs to be processed for reasons of substantial public interest as defined in legislation.

The majority of processing carried out by the Trust will be necessary for the performance of a task carried out in the public interest. As a public authority, it is in the public interest that the Trust operates schools and educates our children. Accordingly, for all the common tasks carried out by the Trust and our schools we do not need to ask for the data subject's consent but rather we can use public interest as our legal basis for processing the appropriate personal data.

This legal basis covers our use of personal data for all the everyday tasks within our schools such as:

- operating a curriculum;
- storing personal data about our students including their parental contacts;
- storing personal data about our staff;
- timetable information;
- cashless catering;
- library systems; and
- the annual census requirements.

However, there could well be some situations where the Trust might need to obtain explicit consent to process personal data or, at the very least, consider whether consent is needed. These could include situations where we share personal data with third party suppliers. If these are for everyday functions of a Trust/school that would be expected by any reasonable person, then 'public interest' may cover this processing. If, on the other hand, the third party supplier is providing a service that might not be expected to be part of everyday school life, then explicit consent would be necessary.

## Consent

Consent must be a positive indication and cannot be inferred from silence, inactivity or pre-ticked boxes. The Trust will only accept consent where it is freely given, specific, 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. With regards to consent, please note:

- the Trust ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data will be found, or the processing will cease;
- consent previously accepted under the Data Protection Act (DPA) will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained;
- consent can be withdrawn by the individual at any time;
- where a student is under the age of 16, 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 student; and
- if consent is our lawful basis for processing personal data when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.

## Individuals Rights

Data subjects (the living individual) that the personal data being processed relates to – have the following rights:

- the right to be informed – this means that individuals must be told what data we are using, why and for what purpose;
- the right of access – individuals have to be allowed to see what data of theirs we are processing if they request it;
- the right of rectification – if data is wrong, we have to correct it;
- the right to erasure – individuals can demand that all data of theirs be erased unless we have a legitimate legal basis for continuing to do so;
- the right to restrict processing – individuals can demand that we stop using their data unless we have a legitimate legal basis for continuing to do so;
- the right to data portability – individuals can decide to move their data to another processor and we have to provide them with all their data so they can do this, however, this only applies to data processed by automated means;
- the right to object – individuals can object to our use of their data and we must stop using it unless we have an overriding legitimate reason to continue; and
- rights in relation to automated decision - making or profiling – individuals can demand that automated decisions about them are reviewed by a human.

## The Right to be Informed (Privacy Notice)

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. If services are offered directly to a child, the Trust 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 or 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; and
- 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.

For data obtained directly from the data subject, this information will be supplied at the time the data is obtained. 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 is disclosed.
- if the data is used to communicate with the individual, at the latest, when the first communication takes place.

**Information to Students and their Families – the "Privacy Notice"**
In order to comply with our data protection obligations, we will inform students and parents/carers of all students of the data we collect, process and hold, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the Local Authority and Department for Education to whom it may be passed. This privacy notice will be passed to students and parents/carers through a specific letter. Parents/carers of new students to our schools will be provided with the privacy notice as part of the admissions process. Our privacy notices can be found in Appendix A and on our websites.

**Information to the Workforce – the "Privacy Notice"**
In order to comply with our data protection obligations, we will inform all staff of the data we collect, process and hold about them, the purposes for which the data is held, our legal basis for doing so, how long we will keep the data for and the third parties such as the Local Authority, Department for Education and HMRC to whom it may be passed. This privacy notice will be passed to staff through a specific letter. New staff joining our Trust will be provided with the privacy notice as part of their contract/induction process. Our Workforce privacy notice can also be found in Appendix A and on our websites.

## The Right of Access (Data Subject Access Requests)

Individuals have the right to obtain confirmation that their data is being processed. Individuals also have the right to submit a Data Subject Access Request (DSAR) to gain access to their personal data in order to verify the lawfulness of the processing. A DSAR will provide the data subject with:

- confirmation that their personal data is being processed;
- access to a copy of the data;
- the purposes of the data processing;
- the categories of personal data concerned;
- who the data has been, or will be, shared with;
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- the source of the data, if not the individual; and
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

When responding to a DSAR:

- we will verify the identity of the person making the request before any information is supplied by asking for two forms of identification;
- we may also contact the individual via phone to confirm the request was made;
- a copy of the information will be supplied to the individual free of charge; however, a 'reasonable fee' may be imposed to comply with requests for further copies of the same information;
- where a DSAR has been made electronically, the information will be provided in a commonly used electronic format;
- where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged;
- all fees will be based on the administrative cost of providing the information;
- 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, 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;
- where a request is manifestly unfounded or excessive, the Trust 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; and
- in the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

When responding to a DSAR we will not disclose information if it:

- might cause serious harm to the physical or mental health of the student or another individual;
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- is contained in adoption or parental order records; or
- is given to a court in proceedings concerning the child.

Data Subject Access Requests must be submitted in writing, either by letter or email to the DPO. They should include:

- the name of the individual;
- the correspondence address;
- a contact number and email address; and
- details of the information requested

If staff receive a DSAR they must immediately forward it to the DPO.

**Children and Data Subject Access Requests**
Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Primary Schools: Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students below the age of 12 **may** be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

Secondary Schools: Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students aged 12 and above **may not** be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

**Parental requests to see the educational record**
There is no automatic parental right of access to the educational record in academies and free schools. To request this, parents should make a Data Subject Access Request as set out above.

## 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, we will inform them of the rectification where possible. Where appropriate, we will inform the individual 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 two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, 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 a judicial remedy.

## 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; and
- the personal data is processed in relation to the offer of information society services to a child.

We have 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; and
- 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, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

## The Right to Restrict Processing

Individuals have the right to block or suppress the Trust's processing of personal data.

In the event that processing is restricted, the Trust 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.

The Trust 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 we have verified the accuracy of the data;
- where an individual has objected to the processing and the Trust is considering whether their legitimate grounds override those of the individual;
- where processing is unlawful and the individual opposes erasure and requests restriction instead; and
- where the Trust 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, we will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

Individuals will be informed when a restriction on processing has been lifted.

## 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 ICT environment to another in a safe and secure manner, 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 and processing is carried out by automated means.

Personal data will be provided in a structured, commonly used and machine-readable form free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual. We are 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, we will consider whether providing the information would prejudice the rights of any other individual.

We will respond to any requests for portability within one month. 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.

Where no action is being taken in response to a request, we 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.

## The Right to Object

We 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.

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; and
- 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; and
- we will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where we 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:

- we will stop processing personal data for direct marketing purposes as soon as an objection is received; and
- we 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; and
- where the processing of personal data is necessary for the performance of a public interest task, we are 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, we will offer a method for individuals to object online.

## 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; and
- it produces a legal effect or a similarly significant effect on the individual.

We 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.

When automatically processing personal data for profiling purposes, we 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; and
- 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:

- we have the explicit consent of the individual; or
- the processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

## Data Protection Impact Assessments (DPIAs)

We have adopted a privacy by design approach and are committed to implementing technical and organisational measures which demonstrate how we have considered and integrated data protection into our processing activities.

When planning to use new technologies and/or the processing is likely to result in a high risk to the rights and freedoms of individuals a Data Protection Impact Assessment (DPIA) will be carried out. DPIAs will be used to identify the most effective method of complying with our data protection obligations and meeting individuals' expectations of

privacy. DPIAs will allow us to identify and resolve problems at an early stage. Where it isn't clear whether a DPIA is required, our Data Protection Officer recommends that one is completed as it is a useful tool to help to ensure compliance with data protection law.

The following criteria should be considered when deciding whether a DPIA is needed. In most cases, meeting two criteria would require a DPIA, but a DPIA may still be completed for a processing operation meeting only one of these criteria. The criteria are:

- evaluation or scoring;
- automated decision making with legal or similar significant effect;
- systematic monitoring;
- sensitive data or data of a highly personal nature;
- data processed on a large scale;
- matching or combining datasets;
- data concerning vulnerable data subjects;
- innovative use or applying new technological or organisational solutions; and
- when the processing in itself prevents data subjects from exercising a right or using a service or contract.

Examples of high risk processing include 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 and the use of CCTV.

We 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; and
- the measures implemented in order to address risk.

## 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.

Heads and Senior Leadership Teams will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training. All staff members must ensure that suspected breaches are reported to our DPO immediately.

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

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

In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, we will notify those concerned directly. A ‘high risk’ breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

Effective and robust breach detection, investigation and internal reporting procedures are in place across the Trust, 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; and
- where appropriate, a description of the measures taken to mitigate any possible adverse effects.

Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

## Security

Security is paramount to all data processing throughout the Prince Albert Community Trust and all staff are required to ensure that all personal/sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period:

- paper records containing personal/sensitive information must not be left unattended or in clear view anywhere with general access;
- paper records containing personal/sensitive information must be kept in a locked filing cabinet, drawer or safe, with restricted access;
- any personal/sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day;
- file cabinets containing personal/sensitive information must be kept closed and locked when not in use or when not attended;
- keys used for access to personal/sensitive information must not be left at an unattended desk;
- computer workstations must be locked when workspace is unoccupied;
- computer workstations must be shut completely down at the end of the work day;
- digital data stored on local hard drives and network drives are controlled by security access lists, and further encrypted or password-protected where necessary and are regularly backed up off-site;
- where data is saved on removable storage or a portable device (such as laptops and tablets), the device must be kept in a locked filing cabinet, drawer or safe when not in use;
- memory sticks must not be used to hold personal information unless they are password-protected and fully encrypted - data from our systems will only be writeable to Trust owned and encrypted USB memory sticks;
- all electronic devices are password-protected to protect the information on the device in case of theft;
- where possible, we enable electronic devices to allow the remote blocking or deletion of data in case of theft;
- staff will not use their personal laptops or computers for school purposes when processing personal data;
- all necessary members of staff are provided with their own secure login and password, and every computer regularly prompts users to change their password;
- passwords must not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location;
- emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient;
- circular emails, (i.e. to parents) are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients;
- when sending confidential information by fax, staff will always check that the recipient is correct before sending;
- where personal/sensitive/confidential information 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 premises accepts full responsibility for the security of the data;
- before sharing data, all staff members will ensure:
    - that they are allowed to share it;
    - that adequate security is in place to protect it; and
    - that those who will be receiving the data have been outlined in a privacy notice.
- under no circumstances are visitors allowed access to personal/sensitive/confidential information;
- visitors to areas of the school containing sensitive information must be supervised at all times;
- printouts containing personal/sensitive information should be sent to the printer as a private print job and immediately removed from the printer upon release/printing;
- whiteboards containing personal/sensitive information should be erased;
- upon disposal personal/sensitive/confidential documents should be shredded
- the physical security of the school's buildings and storage systems, and access to them, is regularly reviewed. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place; and
- the Prince Albert Community Trust takes its Data Protection duties seriously and any unauthorised disclosure may result in disciplinary action.

## Publication of Information

We publish a publication scheme on our website outlining the classes of information that will be made routinely available, including:

- who we are and what we do;
- what we spend and how we spend it;
- what our priorities are and how we are doing;
- how we make decisions;

- our policies and procedures;
- lists and registers; and
- the services we offer.

Classes of information specified in the publication scheme are made available quickly and easily on request. For more information, please see the Trust Freedom of Information Policy & Publication Scheme.

We will not publish any personal information, including photos, on our website(s) without the permission of the affected individual. When uploading information to our website(s), staff are considerate of any metadata or deletions which could be accessed in documents and images on the site. For more information, please see the Trust School Information Published on a Website Policy.

## Photographs and Videos

We understand that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles. We will always indicate our intentions for taking photographs of students and will obtain written permission before publishing them.

Primary schools: we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Secondary schools: we will obtain written consent from parents/carers, or students aged 16 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials. Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the images or video footage and not distribute them further.

Please see the Trust Online Safety Policy for more information on our use of photographs and videos.

## Biometric Recognition Systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students at Prince Albert High School may use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. We will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners by using a PIN code to authorise each transaction if they wish as an alternative to using a finger print.

Parents/carers and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and we will delete any relevant data already captured.

*Please note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18*.

## CCTV

We use CCTV in various locations around our school sites to ensure that they remain safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

For more information, please see the Trust CCTV Policy and direct any enquiries regarding the CCTV systems to the Director of Estates.

## Data Retention and Disposal

Personal data will not be kept for longer than is necessary and will be disposed of securely as soon as practicable. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on our behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Some educational records relating to former students 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.

We have adopted the Information Management Toolkit for Schools created by the IRMS (Information and Records Management Society) and adhere to its principles and guidance.

## Training and Awareness

All staff will receive data protection and privacy training and will be made aware of their responsibilities, as described in this policy through:

- induction training for new staff;
- annual staff training;
- staff meetings / briefings;
- day to day support and guidance from the DPO, the Business Leaders and ICT Support.

Additional training will also be provided as part of continuing professional development, where changes to legislation, guidance or our own processes make it necessary.

## Related Policies

This policy should be read in conjunction with the following policies:

- Trust Freedom of Information Policy & Publication Scheme;
- Trust Technical Security Policy;
- Trust Online Safety Policy;
- Trust Social Media Policy; and
- Trust School Information Published on a Website Policy.

Staff may also find it useful to access the Trust Data Protection and Privacy Internal Toolkit alongside this policy.

## Monitoring and Review

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually, or more regularly in the light of any significant new developments or in response to changes in guidance.

## Appendix A: Privacy Notices

The following pages contain the Prince Albert Community Trust Privacy Notices.

# Privacy Notice

## for parents and carers – use of your personal data

# Contents

# 1. Introduction

Under data protection law, individuals have a right to be informed about how our trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. **This privacy notice explains how we collect, store and use personal data about parents and carers of pupils at our schools.**

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

# 2. The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details and contact preferences (such as your name, address, email address and telephone numbers);
- bank details;
- details of your family circumstances;
- details of any safeguarding information including court orders or professional involvement;
- records of your correspondence and contact with us; and
- details of any complaints you have made.

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- any health conditions you have that we need to be aware of; and
- photographs and CCTV images captured in school.

We may also hold data about you that we have received from other organisations, including other schools and social services.

# 3. Why we use this data

We use the data listed above to:

a) report to you on your child's attainment and progress;
b) keep you informed about the running of school (such as emergency closures) and events;
c) process payments for school services, clubs, trips etc.;
d) provide appropriate pastoral care;
e) protect pupil welfare;
f) assess the quality of our services;
g) administer admissions waiting lists; and
h) comply with our legal and statutory obligations.

**Automated decision making and profiling**

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

# 4. Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

For the purposes of a, b, d, e, f, g and h from section 3 above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school.

For the purposes of d, e, g and h from section 3 above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

For the purposes of d and h from section 3 above, in accordance with the 'consent' basis – we will obtain consent from you to use your personal data.

For the purposes of c from section 3 above, in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you or to help you enter into a contract with us.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

**Our basis for using special category data**
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- we have obtained your explicit consent to use your personal data in a certain way;
- we need to perform or exercise an obligation or right in relation to employment, social security or social protection law;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for the establishment, exercise or defence of legal claims;
- we need to process it for reasons of substantial public interest as defined in legislation;
- we need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- we need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- we need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- we have obtained your consent to use it in a specific way;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- we need to process it for reasons of substantial public interest as defined in legislation.

## 5. Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- local authorities;
- your children;
- government departments or agencies; and
- police forces, courts, tribunals.

## 6. How we store this data

We keep personal information about you while your child is attending our school. We may also keep it beyond their attendance at our school if this is necessary.

Personal data is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- our local authority (Birmingham LA) – to meet our legal obligations to share certain information with it, such as safeguarding concerns, information about exclusions and statutory duties under the Schools Admissions Code including conducting Fair Access Panels;
- government departments or agencies such as the DfE - to meet the statutory duties and legal obligations placed upon us by the Department for Education such as School Census collections under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- our regulator, Ofsted – to assess the quality of our services;
- suppliers and service providers (i.e. external catering providers/cashless catering and payment processors) - to enable them to provide the service we have contracted them for;
- financial organisations (including debt collection agencies);
- our auditors;
- the NHS and health authorities;
- security organisations;
- health and social welfare organisations;
- professional advisers and consultants;
- charities and voluntary organisations; and
- police forces, courts, tribunals.

## 8. Your rights

**How to access personal information that we hold about your child**

You have a right to make a 'Data Subject Access Request' (DSAR) to gain access to personal information that we hold about you.

If you make a DSAR, and if we do hold information about you, we will (subject to any exemptions that apply):

- give you a description of it;
- tell you why we are holding and processing it, and how long we will keep it for;
- explain where we got it from, if not from you;
- tell you who it has been, or will be, shared with;
- let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

**Your other rights regarding your data**

Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- object to our use of your personal data;
- prevent your data being used to send direct marketing;
- object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person);
- in certain circumstances, have inaccurate personal data corrected;
- in certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing;
- in certain circumstances, be notified of a data breach;
- make a complaint to the Information Commissioner's Office; and
- claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk

# Privacy Notice

## for parents and carers – use of your child's personal data

# Contents

# 1. Introduction

Under data protection law, individuals have a right to be informed about how our trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. **This privacy notice explains how we collect, store and use personal data about pupils at our schools.**

This privacy notice applies while we believe your child is not capable of understanding and exercising their own data protection rights.

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), you should instead refer to our privacy notice for pupils to see what rights they have over their own personal data.

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

# 2. The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about your child includes, but is not restricted to:

- contact details, contact preferences, date of birth, identification documents;
- results of internal assessments and externally set tests e.g. national curriculum assessment results;
- pupil and curricular records;
- behaviour and exclusion information e.g. number of temporary exclusions;
- attendance information e.g. number of absences and absence reasons;
- safeguarding information; and
- details of any support received, including care packages, plans and support providers.

We may also collect, use, store and share (when appropriate) information about your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- any medical conditions we need to be aware of, including physical and mental health;
- photographs and CCTV images captured in school; and
- characteristics, such as ethnic background or special educational needs (SEND).

We may also hold data about your child that we have received from other organisations, including other schools and social services.

# 3. Why we use this data

We use the data listed above to:

a) support pupil learning;
b) monitor and report on pupil progress;
c) provide appropriate pastoral care;
d) meet your child's Inclusion needs;
e) protect pupil welfare and keep children safe;
f) assess the quality of our services;
g) administer admissions waiting lists;
h) monitor the use of information and communication technologies;
i) enable your child to participate in offsite activities;
j) comply with the law regarding data sharing; and
k) to meet the statutory duties placed upon us by the Department for Education.

**Automated decision making and profiling**

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

# 4. Our lawful basis for using this data

Our lawful bases for processing your child's personal data for the purposes listed in section 3 above are as follows:

For the purposes of a, b, c, d, e, f, g, h and k from section 3 above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school.

For the purposes of d, e, g, j and k from section 3 above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

For the purposes of d, i and j from section 3 above, in accordance with the 'consent' basis – we will obtain consent from you to use your child's personal data.

Where you have provided us with consent to use your child's data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

**Our basis for using special category data**
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- we have obtained your explicit consent to use your child's personal data in a certain way;
- we need to perform or exercise an obligation or right in relation to employment, social security or social protection law;
- we need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for the establishment, exercise or defence of legal claims;
- we need to process it for reasons of substantial public interest as defined in legislation;
- we need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- we need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- we need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- we have obtained your consent to use it in a specific way;
- we need to protect an individual's vital interests (i.e. protect your child's life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- we need to process it for reasons of substantial public interest as defined in legislation.

## 5. Collecting this data

While the majority of information we collect about your child is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about your child will come from you, but we may also hold data about your child from:

- local authorities;
- previous schools/trusts attended;
- government departments or agencies; and
- police forces, courts, tribunals.

## 6. How we store this data

We keep personal information about your child while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary.

Personal data relating to PACT pupils is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your child's personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your child's personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about your child with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about your child with:

- our local authority (Birmingham LA) – to meet our legal obligations to share certain information with it, such as safeguarding concerns, information about exclusions and statutory duties under the Schools Admissions Code including conducting Fair Access Panels;
- government departments or agencies such as the DfE - to meet the statutory duties and legal obligations placed upon us by the Department for Education such as School Census collections under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- our youth support services provider (for pupils aged 13+, see more information below);
- educators and examining bodies;
- our regulator, Ofsted – to assess the quality of our services;
- suppliers and service providers (i.e. external catering providers) - to enable them to provide the service we have contracted them for;
- financial organisations (including debt collection agencies);
- our auditors;
- the NHS and health authorities;
- security organisations;
- health and social welfare organisations;
- professional advisers and consultants;
- police forces, courts, tribunals; and
- pupils' destinations upon leaving one of our schools.

The information that we share with these parties may include the following:

- safeguarding files;
- contact information;
- teaching and learning information including assessments; and
- SEND information.

**National Pupil Database**
We are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with third parties, such as other organisations which promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

**Youth support services – pupils aged 13+**
Once pupils reach the age of 13, we also pass pupil information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- youth support services; and
- careers advisers.

A parent or guardian can object to any information in addition to their child's name, address and date of birth being passed to their local authority or provider of youth support services by informing us. This right is transferred to the pupil once they reach the age 16.

**Youth support services – pupils aged 16+**
We will also share certain information about pupils aged 16+ with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services; and
- careers advisers.

A pupil once they reach the age of 16 can object to only their name, address and date of birth being passed to their local authority or provider of youth support services by informing us.

# 8. Your rights

**How to access personal information that we hold about your child**
You have a right to make a 'Data Subject Access Request' (DSAR) to gain access to personal information that we hold about your child.

If you make a DSAR, and if we do hold information about your child, we will (subject to any exemptions that apply):

- give you a description of it;
- tell you why we are holding and processing it, and how long we will keep it for;
- explain where we got it from, if not from you;
- tell you who it has been, or will be, shared with;
- let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- give you a copy of the information in an intelligible form.

You may also have the right for your child's personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your child for you to make a subject access request on their behalf.

**Your right to access your child's educational record**
There is no automatic parental right of access to the educational record in academies and free schools. To request this, parents should make a Data Subject Access Request as set out above.

**Your other rights regarding your child's data**
Under data protection law, you have certain rights regarding how your child's personal data is used and kept safe. For example, you have the right to:

- object to our use of your child's personal data;
- prevent your child's data being used to send direct marketing;
- object to and challenge the use of your child's personal data for decisions being taken by automated means (by a computer or machine, rather than by a person);
- in certain circumstances, have inaccurate personal data corrected;
- in certain circumstances, have the personal data we hold about your child deleted or destroyed, or restrict its processing;
- in certain circumstances, be notified of a data breach;
- make a complaint to the Information Commissioner's Office; and
- claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

Once your child is able to understand their rights over their own data (generally considered to be age 12, but this has to be considered on a case-by-case basis), we will need to obtain consent from your child for you to make these requests on their behalf.

# 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk

# Privacy Notice

## for pupils – use of your personal data

# Contents

# 1. Introduction

You have a legal right to be informed about how our trust uses any personal information that we hold about you. To comply with this, we provide a 'privacy notice' to you where we are processing your personal data. **This notice explains how we collect, store and use personal data about pupils at our school, like you.**

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

# 2. The personal data we hold

We hold some personal information about you to make sure we can help you learn and look after you at school.

For the same reasons, we get information about you from some other places too – like other schools, the local council and the government.

Personal information that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- your contact details, date of birth, identification documents;
- your test results;
- your attendance records;
- details of any behaviour issues or exclusions;
- safeguarding information; and
- details of any additional support received.

We may also collect, use, store and share (when appropriate) information about your child that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- any medical conditions you have;
- photographs and CCTV images captured in school; and
- your characteristics, such as ethnic background or special educational needs (SEND).

# 3. Why we use this data

We use the data listed above to:

a) get in touch with you and your parents when we need to;
b) check how you're doing in school and your progress (such as in tests and exams) and to work out whether you or your teachers need any extra help;
c) to look after your wellbeing and keep you safe;
d) track how well the school/trust as a whole is performing;
e) monitor the use of ICT;

**Automated decision making and profiling**

We don't currently put your personal information through any automated decision making or profiling process. This means we don't make decisions about you using only computers without any human involvement. If this changes in the future, we will update this notice in order to explain the processing to you, including your right to object to it.

# 4. Our lawful basis for using this data

We will only collect and use your information when the law allows us to. We need to establish a 'lawful basis' to do this. Our lawful bases for processing your personal information for the reasons listed in section 3 above are:

For the purposes of a, b, c, d and e from section 3 above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school.

For the purposes of c from section 3 above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

Where you've provided us with consent to use your information, you may take back this consent at any time. We'll make this clear when requesting your consent, and explain how you'd go about withdrawing consent if you want to.

**Our basis for using special category data**
For 'special category' data (more sensitive personal information), we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- we have obtained your explicit consent to use your information in a certain way;
- we need to use your information under employment, social security or social protection law;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the information has already been made obviously public by you;
- we need to use it to make or defend against legal claims;
- we need to use it for reasons of substantial public interest as defined in legislation;
- we need to use it for health or social care purposes, and it's used by, or under the direction of, a professional obliged to confidentiality under law;
- we need to use it for public health reasons, and it's used by, or under the direction of, a professional obliged to confidentiality under law;
- we need to use it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the use is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- we have obtained your consent to use it in a specific way;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made obviously public by you;
- we need to use it as part of legal proceedings, to obtain legal advice, or to make or defend against legal claims;
- we need to process it for reasons of substantial public interest as defined in legislation.

## 5. Collecting this data

While most of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we want to collect information from you, we make it clear if you have to give us this information (and if so, what the possible consequences are of not doing that), or if you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- local authorities;
- previous schools/trusts attended;
- government departments or agencies; and
- police forces, courts, tribunals.

## 6. How we store this data

We keep personal information about you while you're attending our school. We may also keep it beyond your attendance at our school if this is necessary.

Personal data relating to PACT pupils is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about you with any third party without your consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- our local authority (Birmingham LA) – to meet our legal obligations to share certain information with it, such as safeguarding concerns and information about exclusions;

- government departments or agencies such as the DfE - to meet the statutory duties and legal obligations placed upon us by the Department for Education such as School Census collections under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013;
- our youth support services provider (for pupils aged 13+, see more information below);
- educators and examining bodies;
- our regulator, Ofsted – to assess the quality of our services;
- suppliers and service providers (i.e. external catering providers) - to enable them to provide the service we have contracted them for;
- financial organisations;
- our auditors;
- the NHS and health authorities;
- security organisations;
- health and social welfare organisations;
- professional advisers and consultants;
- police forces, courts, tribunals; and
- your destination upon leaving one of our schools.

The information that we share with these parties may include the following:

- safeguarding files;
- contact information;
- teaching and learning information including assessments; and
- SEND information.

**National Pupil Database**

We are required to provide information about you to the Department for Education (a government department) as part of data collections such as the school census.

Some of this information is then stored in the National Pupil Database (NPD), which is owned and managed by the Department for Education and provides evidence on school performance to inform research.

The database is held electronically so it can easily be turned into statistics. The information is securely collected from a range of sources including schools, local authorities and exam boards.

The Department for Education may share information from the NPD with third parties, such as other organisations which promote children's education or wellbeing in England. These third parties must agree to strict terms and conditions about how they will use the data.

For more information, see the Department's webpage on how it collects and shares research data.

You can also contact the Department for Education with any further questions about the NPD.

**Youth support services – age 13+**

Once you reach the age of 13, we also pass your information to our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services to you as follows:

- youth support services; and
- careers advisers.

Your parent or guardian can object to any information in addition to your name, address and date of birth being passed to the local authority or provider of youth support services by informing us. This right is transferred to you once you reach the age of 16.

**Youth support services - age 16+**

We will also share certain information about you when you reach the age of 16 with our local authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services; and
- careers advisers.

Once you reach the age of 16 you can only object to your name, address and date of birth being passed to the local authority or provider of youth support services. You can do this by informing us.

## 8. Your rights

**How to access personal information that we hold about your child**
You have a right to make a 'Data Subject Access Request' (DSAR) to gain access to personal information that we hold about you.

If you make a DSAR, and if we do hold information about you, we will (unless there's a really good reason why we shouldn't):

- give you a description of it;
- tell you why we are holding and using it, and how long we will keep it for;
- explain where we got it from, if not from you;
- tell you who it has been, or will be, shared with;
- let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- give you a copy of the information in an understandable form.

You may also have the right for your personal information to be shared electronically with another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

**Your other rights regarding your data**
Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- say that you don't want your personal information to be used;
- stop it being used to send you marketing materials;
- say that you don't want it to be used for automated decisions (decisions made by a computer or machine, rather than by a person);
- in some cases, have it corrected if it's inaccurate;
- in some cases, have it deleted or destroyed, or restrict its use;
- in some cases, be notified of a data breach;
- make a complaint to the Information Commissioner's Office; and
- claim compensation if the data protection rules are broken and this harms you in some way.

To exercise any of these rights, please contact us (see 'Contact us' below).

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please let us know first (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk

# Privacy Notice

## for our Workforce

# Contents

# 1. Introduction

Under data protection law, individuals have a right to be informed about how our Trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data.

This privacy notice explains how we collect, store and use personal data about individuals we employ, or otherwise engage to work at our Trust.

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

# 2. Data processing

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details;
- date of birth, marital status and gender;
- next of kin and emergency contact numbers;
- salary, annual leave, pension and benefits information;
- bank account details, payroll records, National Insurance number and tax status information;
- recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process;
- qualifications and employment records, including work history, job titles, working hours, training records and professional memberships;
- performance information;
- outcomes of any disciplinary and/or grievance procedures;
- absence data;
- copy of driving licence; and
- data regarding your use of the Trust's information and communications technologies.

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to, information about:

- any health conditions you have that we need to be aware of;
- sickness records;
- photographs and CCTV images captured in school; and
- trade union membership.

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.

We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

# 3. Why we use this data

We use the data listed above to:

a) Enable you to be paid
b) Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
c) Support effective performance management
d) Inform our recruitment and retention policies
e) Allow better financial modelling and planning
f) Enable equalities monitoring
g) Improve the management of workforce data across the sector
h) Support the work of the School Teachers' Review Body

**Automated decision making and profiling**

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

## 4. Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

For the purposes of b, c, d, e, f, g and h in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school.

For the purposes of a, b and c in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

For the purposes of a, b and c in accordance with the 'contract' basis – we need to process personal data to fulfil a contract with you or to help you enter into a contract with us.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds which justify the use of your data. For example, we will gain your consent to use your photograph for any reason other than for safeguarding purposes; for example displaying your photograph on the school website or in the staff journal.

**Our basis for using special category data**
For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- we have obtained your explicit consent to use your personal data in a certain way;
- we need to perform or exercise an obligation or right in relation to employment, social security or social protection law;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for the establishment, exercise or defence of legal claims;
- we need to process it for reasons of substantial public interest as defined in legislation;
- we need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- we need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- we need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- we have obtained your consent to use it in a specific way;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- we need to process it for reasons of substantial public interest as defined in legislation.

## 5. Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice. For example:

- Employment checks: failure to provide the school with ample proof of a right to work in the UK will prevent employment with the organisation. Employees found to be working illegally could face prosecution by law enforcement officers.
- Salary requirements: failure to provide accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or an employee paying too much tax.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- local authorities;
- government departments or agencies; and
- police forces, courts, tribunals.

## 6. How we store this data

We keep personal information about you while you work at our Trust. We may also keep it beyond your employment at our Trust if this is necessary.

Personal data relating to staff is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- our local authority (Birmingham) – to meet our legal obligations to share certain information with it, such as safeguarding concerns;
- government departments or agencies;
- our regulator, Ofsted;
- suppliers and service providers:
- List the specific types of providers – to enable them to provide the service we have contracted them for, such as payroll / HR / legal;
- financial organisations including debt collection agencies;
- our auditors;
- survey and research organisations;
- health authorities;
- Trade Unions and associations;
- your family or representatives;
- security organisations;
- health and social welfare organisations;
- professional advisers and consultants;
- charities and voluntary organisations;
- Police forces, courts, tribunals

## 8. Your rights

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

**How to access personal information that we hold about you**

You have a right to make a 'Data Subject Access Request' (DSAR) to gain access to personal information that we hold about you.

If you make a DSAR, and if we do hold information about you, we will (subject to any exemptions that apply):

- give you a description of it;
- tell you why we are holding and processing it, and how long we will keep it for;
- explain where we got it from, if not from you;
- tell you who it has been, or will be, shared with;
- let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

**Your other rights regarding your data**
Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- object to our use of your personal data;
- prevent your data being used to send direct marketing;
- object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person);
- in certain circumstances, have inaccurate personal data corrected;
- in certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing;
- in certain circumstances, be notified of a data breach;
- make a complaint to the Information Commissioner's Office; and
- claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk

**Please see overleaf for the declaration that you must return to school as soon as possible.**

## PACT Workforce Data Protection & Privacy Declaration

I, (name) _____, declare that I understand:

- that the PACT has a legal and legitimate interest to collect and process my personal data in order to meet statutory and contractual requirements;
- there may be significant consequences if I fail to provide the personal data the PACT requires;
- that the PACT may share my data with the DfE, and subsequently the LA;
- that the PACT will not share my data with any third parties without my consent, unless the law and PACT policies allow them to do so;
- the nature and personal categories of this data, and where the personal data originates from (where the data is obtained from third parties);
- my data is retained in line with the PACT Data Protection and Privacy policy; and
- my rights with regards to the processing of my personal data.

Furthermore, I understand that as an employee of the PACT, I have an obligation to:

- inform the Data Protection Officer (DPO) of any Data Subject Access Request (DSAR) I receive (for example, from a parent) immediately;
- inform the Data Protection Officer (DPO) of any suspected data breach as soon as I become aware of it;
- adhere to the PACT Data Protection and Privacy policy.

**Full name:** _____ **Signature:** _____ **Date:** _____ / _____ / _____

## PACT Workforce Photograph/Video Consent Form

Please ensure you complete all of the following statements.

| | | |
|---|---|---|
| I consent to photographs of me being published (other than for safeguarding purposes). For example, in newsletters, displays, the staff journal, websites, twitter etc. | | |
| **Please tick** | **Yes** _____ | **No** _____ |
| I consent to videos of me being published (other than for safeguarding purposes). For example, in newsletters, displays, the staff journal, websites, twitter etc. | | |
| **Please tick** | **Yes** _____ | **No** _____ |

**Full name:** _____ **Signature:** _____ **Date:** _____ / _____ / _____

Please remember that you have the right to withdraw your consent at any time. To do so, please contact the school office and ask for a new PACT Workforce Photograph/Video Consent Form and return the completed form to the school office.

# Privacy Notice

## Governance Board/Committees and Other Volunteers

# Contents

# 1. Introduction

Under data protection law, individuals have a right to be informed about how our trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. This privacy notice explains how we collect, store and use personal data about individuals working with our trust in a voluntary capacity, including Academy Committee Representatives and Trustees.

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

# 2. The personal data we hold

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details;
- references;
- evidence of qualifications;
- employment details; and
- information about business and pecuniary interests.

We may also collect, use, store and share (when appropriate) information about you that falls into "special categories" of more sensitive personal data. This includes, but is not restricted to:

- information about any health conditions you have that we need to be aware of;
- information about disability and access requirements; and
- photographs and CCTV images captured in school.

We may also collect, use, store and share (when appropriate) information about criminal convictions and offences.
We may also hold data about you that we have received from other organisations, including other schools and social services, and the Disclosure and Barring Service in respect of criminal offence data.

# 3. Why we use this data

We use the data listed above to:

a) establish and maintain effective governance;
b) meet statutory obligations for publishing and sharing [representatives'/trustees'] details;
c) facilitate safe recruitment, as part of our safeguarding obligations towards pupils;
d) undertake equalities monitoring;
e) ensure that appropriate access arrangements can be provided for volunteers who require them.

**Automated decision making and profiling**

We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

# 4. Our lawful basis for using this data

Our lawful bases for processing your personal data for the purposes listed in section 3 above are as follows:

For the purposes of a, b, c, d, and e from section 3 above, in accordance with the 'public task' basis – we need to process data to fulfil our statutory function as a school.

For the purposes of a, b, c and e from section 3 above, in accordance with the 'legal obligation' basis – we need to process data to meet our responsibilities under law.

Where you have provided us with consent to use your data, you may withdraw this consent at any time. We will make this clear when requesting your consent, and explain how you would go about withdrawing consent if you wish to do so.

**Our basis for using special category data**

For 'special category' data, we only collect and use it when we have both a lawful basis, as set out above, and one of the following conditions for processing as set out in data protection law:

- we have obtained your explicit consent to use your personal data in a certain way;
- we need to perform or exercise an obligation or right in relation to employment, social security or social protection law;

- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for the establishment, exercise or defence of legal claims;
- we need to process it for reasons of substantial public interest as defined in legislation;
- we need to process it for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law;
- we need to process it for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law;
- we need to process it for archiving purposes, scientific or historical research purposes, or for statistical purposes, and the processing is in the public interest.

For criminal offence data, we will only collect and use it when we have both a lawful basis, as set out above, and a condition for processing as set out in data protection law. Conditions include:

- we have obtained your consent to use it in a specific way;
- we need to protect an individual's vital interests (i.e. protect your life or someone else's life), in situations where you're physically or legally incapable of giving consent;
- the data concerned has already been made manifestly public by you;
- we need to process it for, or in connection with, legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights;
- we need to process it for reasons of substantial public interest as defined in legislation.

## 5. Collecting this data

While the majority of information we collect about you is mandatory, there is some information that can be provided voluntarily.

Whenever we seek to collect information from you, we make it clear whether you must provide this information (and if so, what the possible consequences are of not complying), or whether you have a choice.

Most of the data we hold about you will come from you, but we may also hold data about you from:

- local authorities;
- government departments or agencies; and
- police forces, courts, tribunals.

## 6. How we store this data

We keep personal information about you while you volunteer at our trust. We may also keep it beyond your work at our trust if this is necessary.

Personal data relating to PACT representatives/trustees and volunteers is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

We do not share information about you with any third party without consent unless the law and our policies allow us to do so.

Where it is legally required, or necessary (and it complies with data protection law), we may share personal information about you with:

- our local authority (Birmingham) – to meet our legal obligations to share certain information with it, such as safeguarding concerns;
- government departments or agencies;
- our regulator, Ofsted;
- suppliers and service providers (i.e. HR) - to enable them to provide the service we have contracted them for;
- our auditors;
- health authorities;

- security organisations;
- professional advisers and consultants;
- police forces, courts, tribunals; and
- charities and voluntary organisations.

## 8. Your rights

**How to access personal information that we hold about you**
You have a right to make a 'Data Subject Access Request' (DSAR) to gain access to personal information that we hold about you.

If you make a DSAR, and if we do hold information about you, we will (subject to any exemptions that apply):

- give you a description of it;
- tell you why we are holding and processing it, and how long we will keep it for;
- explain where we got it from, if not from you;
- tell you who it has been, or will be, shared with;
- let you know whether any automated decision-making is being applied to the data, and any consequences of this; and
- give you a copy of the information in an intelligible form.

You may also have the right for your personal information to be transmitted electronically to another organisation in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

**Your other rights regarding your data**
Under data protection law, you have certain rights regarding how your personal data is used and kept safe. For example, you have the right to:

- object to our use of your personal data;
- prevent your data being used to send direct marketing;
- object to and challenge the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person);
- in certain circumstances, have inaccurate personal data corrected;
- in certain circumstances, have the personal data we hold about you deleted or destroyed, or restrict its processing;
- in certain circumstances, be notified of a data breach;
- make a complaint to the Information Commissioner's Office; and
- claim compensation for damages caused by a breach of the data protection regulations.

To exercise any of these rights, please contact us (see 'Contact us' below).

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our data protection officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk

# PACT Governance Board/Committees and Other Volunteers
# Data Protection & Privacy Declaration

I, (name) _____, declare that I understand:

- that the PACT has a legal and legitimate interest to collect and process my personal data in order to meet statutory requirements;
- there may be consequences if I fail to provide the personal data the PACT requires;
- that the PACT may share my data with the DfE, and subsequently the LA;
- that the PACT will not share my data with any third parties without my consent, unless the law and PACT policies allow them to do so;
- the nature and personal categories of this data, and where the personal data originates from (where the data is obtained from third parties);
- my data is retained in line with the PACT Data Protection and Privacy policy; and
- my rights with regards to the processing of my personal data.

Furthermore, I understand that as a Governance Representative of the PACT, I have an obligation to:

- inform the Data Protection Officer (DPO) of any Data Subject Access Request (DSAR) I receive (for example, from a parent/member of staff) immediately;
- inform the Data Protection Officer (DPO) of any suspected data breach as soon as I become aware of it; and
- adhere to the PACT Data Protection and Privacy policy.

**Full name:** _____ **Signature:** _____ **Date:** _____ / _____ / _____

# Privacy Notice

## for PACT Websites
## (including the use of cookies)

# Contents

# 1. Introduction

Under data protection law, individuals have a right to be informed about how our trust uses any personal data that we hold about them. We comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where we are processing their personal data. **This privacy notice explains how we collect, store and use personal data about visitors to our PACT websites.**

**These websites include:** **www.the-pact.co.uk / www.pact.bham.sch.uk;**
**www.pahigh.co.uk;**
**www.princealbert.bham.sch.uk;**
**www.heathfld.bham.sch.uk;**
**www.hifield.bham.sch.uk;**
**www.birchfld.bham.sch.uk; and**
**www.suttonparkprimary.co.uk**

Prince Albert Community Trust (PACT) is the 'data controller' for the purposes of data protection law.
GDPR Sentry Ltd have been appointed as our data protection officer (see 'Contact us' below).

PACT is the data controller for any pages hosted on the websites above. If you follow a link to a service provided by another school, company, government agency or local authority, that organisation will:

- be the data controller;
- be responsible for processing any data you share with them; and
- publish and manage their own privacy notice with details of how to contact them.

# 2. The personal data we collect

Personal data that we may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- contact details such as your name, email address and telephone number if you contact us via our websites;
- questions, queries or feedback you leave, including your contact details;
- how you use our emails - for example whether you open them and which links you click on;
- your Internet Protocol (IP) address, and details of which version of web browser you used; and
- information on how you use the site, using cookies and page tagging techniques.

Certain PACT websites use Google Analytics software to collect information about how you use them. This includes IP addresses. The data is anonymised before being used for analytics processing.

Google Analytics processes anonymised information about:

- the pages you visit on certain PACT websites;
- how long you spend on each page;
- how you got to the site; and
- what you click on while you're visiting the site.

We do not store your personal information through Google Analytics (for example your name or address).

We will not identify you through analytics information, and we will not combine analytics information with other data sets in a way that would identify who you are.

# 3. Why we use this data

We collect information through Google Analytics to see how you use our sites and services. We do this to help:

- make sure our sites are meeting the needs of our users; and
- make improvements, for example improving the search functionality on our sites.

We also collect data in order to:

- gather feedback to improve our services;
- respond to any feedback or enquiries you send us, if you've asked us to; and
- send email alerts to users who request them (where this functionality is available).

**Automated decision making and profiling**
We do not currently process any personal data through automated decision making or profiling. If this changes in the future, we will amend any relevant privacy notices in order to explain the processing to you, including your right to object to it.

## 4. Our lawful basis for using this data

Our legal basis for processing anonymised data for Google Analytics is your consent.

The legal basis for processing all other personal data is that it's necessary to perform a task in the public interest.

## 5. Use of cookies

Cookies are small text files saved on your phone, tablet or computer when you visit a website.

We use cookies on some of our websites to store information about how you use the website, such as the pages you visit.

On any of our websites which use cookies, you will always be presented with a cookie notification window on your first visit. This window will allow you to choose which cookies you're happy for us to use, and you can change these settings at any time. We currently use 2 types of cookie on some of our websites as detailed below.

**Type 1: strictly necessary cookies**
Necessary cookies enable core functionality such as security, network management, and accessibility. They always need to be on. You may disable these by changing your browser settings, but this may affect how the website functions. These essential cookies also do things like remembering your progress through a form (for example an expression of interest or feedback form).

**Type 2: analytics cookies**
Analytics cookies are cookies that measure website use. We use Google Analytics to measure how you use a website so we can improve it based on user needs. We do not allow Google to use or share the data about how you use the site. Google Analytics sets cookies that store anonymised information about:

- how you got to the site;
- the pages you visit on the site, and how long you spend on each page; and
- what you click on while you're visiting the site.

**Cookies we use**
The table below explains some of the cookies we use and why.

| Cookie | Name | Purpose |
|---|---|---|
| Cookie preference | CookieControl | This cookie is used to remember a user's choice about cookies. Where users have previously indicated a preference, that user's preference will be stored in this cookie. |
| Universal Analytics (Google) | _ga<br>_gali<br>_gat<br>_gid | These cookies are used to collect information about how visitors use our website. We use the information to compile reports and to help us improve the website. The cookies collect information in a way that does not directly identify anyone, including the number of visitors to the website, where visitors have come to the website from and the pages they visited. Read Google's overview of privacy and safeguarding data. |

**How do I change my cookie settings?**
You can change your cookie preferences at any time by clicking on the 'C' icon in the bottom left hand corner of our websites (only available where we use cookies). You can then click 'I Accept' to accept all cookies, 'I Do Not Accept' to reject all cookies, or you can adjust the available sliders to 'On' or 'Off' to personalise your choices, clicking the 'X' to save your choices and close the window. You may need to refresh your page for your settings to take effect.

Alternatively, most web browsers allow some control of most cookies through the browser settings. To find information relating to your web browser, visit the browser developer's website. To find out more about cookies, including how to see what cookies have been set, visit www.aboutcookies.org or www.allaboutcookies.org.

To opt out of being tracked by Google Analytics across all websites, visit http://tools.google.com/dlpage/gaoptout.

## 6. How we store this data

Personal data is stored in line with the PACT Data Protection and Privacy Policy.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed.

We will dispose of your personal data securely when we no longer need it.

## 7. Who we share data with

The data we collect may be shared with government departments, agencies and public bodies. It may also be shared with our technology suppliers, for example our hosting provider.

We will not:

- sell or rent your data to third parties;
- share your data with third parties for marketing purposes.

We will share your data if we are required to do so by law - for example, by court order, or to prevent fraud or other crime.

## 8. Your rights

You have the right to request:

- information about how your personal data is processed;
- a copy of that personal data;
- that anything inaccurate in your personal data is corrected immediately.

You can also:

- raise an objection about how your personal data is processed;
- request that your personal data is erased if there is no longer a justification for it;
- ask that the processing of your personal data is restricted in certain circumstances.

If you would like to make a request, please contact us (see 'Contact us' below).

## 9. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with us in the first instance (see 'Contact us' below).

Alternatively, you can raise a concern directly with the Information Commissioner's Office (ICO). The ICO can be contacted on 0303 123 1113, Monday-Friday 9am-5pm.

## 10. Contact us

If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact our Data Protection Officer detailed below.

Data Protection Officer: GDPR Sentry Ltd
Email: dpo@the-pact.co.uk