ASHMORE PARK

AND

PHOENIX NURSERY SCHOOLS FEDERATION

DATA PROTECTION POLICY

Senior Leadership Team/Compliance Governor(s) Review Date	03.03.2021
Governing Board Approved/Adopted	11.03.2021
Signed on behalf of the Governing Board/Committee	
Policy to be Reviewed Date	31.03.2023

Contents

1. Aims

Ashmore Park and Phoenix Nursery Schools Federation aims to ensure that all personal data collected about staff, children, parents, Governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation.

Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Both schools' in our Federation, processes personal data relating to parents, children, staff, Governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

This policy applies to **all staff** employed across our Federation, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing board

The Governing Board has overall responsibility for ensuring that our Federation complies with all relevant data protection obligations.

5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the Governing Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO service is being provided by the Local Authority under the terms of the Service Level Agreement, which has been purchased, for both individual schools in the Federation. Our DPO is contactable by ringing 01902 555166 or alternatively you can email the Information Governance Manager on:

Anna.Zollino-Biscotti@wolverhampton.gov.uk

5.3 Headteacher

The Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their appropriate School of any changes to their personal data, such as a change of address, name etc.
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

The GDPR is based on data protection principles that our Federation must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the Federation aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Federation/School can **fulfil a contract** with the individual, or the individual has asked the Federation/School to take specific steps before entering into a contract
- The data needs to be processed so that the Federation/school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Federation/School, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Federation/School or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a child) has freely given clear **consent**.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Federation's retention of records schedule.

8. Sharing personal data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a child or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will, however, seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and children, for example, I.T companies such as Teachers2Parents, eServices, DC Pro etc. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share

- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our children or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the Federation holds about them. This includes:

- 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
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests can be submitted verbally or in writing to the Headteacher. Written requests can either be submitted by letter or by email to the DPO. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested.

If staff receive a subject access request they must immediately forward it to the Headteacher who shall contact the DPO for information, advice and guidance.

9.2 Children and 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.

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 children from both schools within our Federation may be granted without the express permission of the child. This is not a rule and a child's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the child 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
- Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs.

A request will be deemed unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area

- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a child) within 15 school days of receipt of a verbal or written request.

11. Biometric recognition systems

The Federation does not currently operate a 'Biometric Recognition System' in either of its schools.

12. CCTV

We use CCTV in various locations around each school site to ensure it remains safe and secure. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to the individual School's Senior Administrator.

13. Photographs and videos

As part of our Federation's activities, we may take photographs and record images of individuals within our 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 the parent/carer.

Uses may include:

- Within school on notice boards, in either of the school prospectus', newsletters, etc.
- Outside of school with regional, national and international professional partners
- Outside of school by external agencies such as newspapers, campaigns etc.
- Online on either school's website or Facebook page(s).

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

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

See Appendices 1 to 3 for further guidance on our specific use of digital media across the Federation. See our Safeguarding and Child Protection Policy for additional information on procedures and processes followed across the Federation to safeguard all children in our care.

14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notice, see Appendix 4)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on show in offices and on classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where personal information needs to be taken off site, staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

- Staff or Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our Employee Code of Conduct and Expected Standards Policy)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. Disposal of records

Personal data that is no longer needed will be disposed of securely. 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 paper-based records, and delete electronic files. We may also use a third party to safely dispose of records on the Federation's behalf. If we do so, we will utilise a Local Authority approved provider to ensure sufficient guarantees are in place and that the provider complies with data protection law.

17. Personal data breaches

The Federation will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 5.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of children eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about children.

18. Training

All staff and Governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Federation's processes make it necessary.

19. Monitoring arrangements

The DPO and the Governing Board's nominated Compliance Link Governors are responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law (as the Data Protection Act 2018) or if any changes are made to the bill that affect our Federation's practice. Otherwise, or from then on, this policy will be reviewed every two years and presented to the Governing Board for approval.

20. Links with other policies

This data protection policy is linked to our:

- Digital Safeguarding Policy
- Employee Code of Conduct and Expected Standards Policy

- Governor Visit Policy
- Safeguarding and Child Protection Policy
- Supporting Pupils with Medical Needs Policy.

Appendix 1: Example of a Pupil Profile Document used within the Federation

PUPIL PROFILE

CHILD'S NAME: .....

In the event that we the need to contact someone regarding your child e.g. they may be sick or had an accident, please list the people you would like us to contact, in the order of preference.

Please be advised that you must ensure that you obtain consent from each 'Individual Contact' prior to disclosing their personal contact details.

	Contact 1	Contact 2	Contact 3	Contact 4
Name of Contact				
Relationship to Child				
Home Telephone Number				
Mobile Telephone Number				
Work Telephone Number ***(Where Applicable)***				

Please note that there may be a time, in exceptional circumstances or in the event of an emergency, where contact by telephone cannot be obtained. The responsibility, therefore, for arranging emergency treatment for your child/ren would be delegated to the staff at this School.

WHY WE ARE ASKING FOR CONSENT:

In line with the Data Protection Act 2018 (GDPR), we are requesting your consent in regards to the following:

a. **A suspected outbreak of head lice**

I give consent for a member of staff to check my child's hair in the event of a suspected outbreak of head lice in the School

YES	NO

b. Taking your child out of School grounds for a visit within the locality

I give consent for my child to be taken out of the School grounds for a visit within the locality providing Local Authority policies for supervision are observed

YES	NO

c. The School's Website and Facebook page

I give consent for photographs of my child engaging in learning activities either individually or in groups to be used on the School website and Facebook page

YES	NO

d. Contact Permissions

We understand that the School uses 'Teachers2Parents' and 'Microsoft Teams' to send out information or reminder texts, or to share information about our child's learning, information received may include:

- Arrangements due to bad weather or staff training days
- A reminder to return Library Books to School
- A prompt to return permission slips when Fundraising or attending School Trips
- A deadline to return School Photograph monies for courier collection
- A reminder that voluntary School Fund donations are due for payment.

In order to provide the 'Teachers2Parents' service we use the nominated parent/carer's mobile telephone number and 'Microsoft Teams' will be activated using the nominated parent/carer's email address.

I give consent for the School to utilise my mobile telephone number for the 'Teachers2Parents' text messaging service and to utilise my email address for the purposes of information sharing via the 'Microsoft Teams App'

YES	NO

N.B: Please note that your child's 'Microsoft Teams Account' will remain 'live' until 31 December to allow you time to print any photographs etc. after this date the account will be closed to all users and permanently deleted.

I give consent for my child's Educator to share photographs of my child engaging in learning activities, either individually or in groups, via the 'Microsoft Teams App'

YES	NO

Please note that you are free to withdraw your consent at any time, this can be done by emailing ashmoreparknurseryschool@wolverhampton.gov.uk; by calling 01902 558116 or by visiting the School office.

Signed: ..... Date: .....

Appendix 2: Example of a Local/Regional/National/International Learning Network Document used within the Federation

LOCAL/REGIONAL/NATIONAL/INTERNATIONAL LEARNING NETWORKS

SECTION (A) – LEARNING NETWORK OUTLINE:

The Federation is a member of a learning network, which is considered normal practice for both schools within the Federation, these learning networks, may be local; regional or international.

In order for this to be a purposeful learning experience for all, we will share our observations of what children do and say, and will share the documentation of our work with a wider audience than the staff, and families of this school.

SECTION (B) – HOW DIGITAL MEDIA IS UTILISED BOTH INTERNALLY/EXTERNALLY WITH PROFESSIONAL PARTNERS:

- The use of digital media is an integral part of the documentation process and as such we would like to share images/recordings with our colleagues from other settings, please note that all images are anonymised and will not include your child's name, date of birth etc.
- As part of the Federation's vision for its school's and as a Professional Learning Environment, school documentation, which may include images or recordings demonstrating the work of the children, may be shared locally, regionally, nationally and internationally to showcase outstanding Early Years practices
- It is important to understand that if you give consent, the school may utilise documentation, which could include images or recordings of your child, which will exceed your child's time at this school.

WHY WE ARE REQUESTING YOUR CONSENT:

In line with the Data Protection Act 2018 (GDPR), we are requesting your consent (*please see Parent Declaration overleaf), to use School documentation which could include images/recordings of your child for the purposes outlined above.

If you are not happy for images/recordings of your child to be included, this will not prevent them from participating in future projects, we will, however, ensure that no images that identify your child are used in any of the documentation.

**NB. Please see Parent Declaration overleaf*

PARENT DECLARATION:

Please read the statements below and tick YES to give your consent or NO if you do not give your consent to the following:

I give permission for images/recordings of my child to be included in documentation we share as part of our local, regional, national and international learning networks and understand that this information may be held by the school for a period of time which will exceed my child's time at the school

YES	NO

I give permission for images/recordings of my child, to be used to promote the School i.e. to be included in the School prospectus or promotional materials, to be used in research papers, or other professional publications, which may be shared with local, regional, national and/or international audiences

YES	NO

Please note that you are free to withdraw your consent at any time, this can be done by emailing ashmoreparknurseryschool@wolverhampton.gov.uk; by calling 01902 558116 or by visiting the School office.

In all instances, we would urge you to discuss any concerns that you may have with your child's Educator or Headteacher.

Child's Name: ..... Date: .....

Signature of Parent/Carer: .....

Appendix 3: Privacy Notice

ASHMORE PARK AND PHOENIX NURSERY SCHOOLS FEDERATION

PRIVACY NOTICE – CHILDREN'S INFORMATION

The categories of children's information that we collect, hold and share includes:

- Personal information (such as name, date of birth, Unique Pupil Number (UPN), address, parents/carer's details, medical conditions, special educational needs information etc.)
- Characteristics (such as ethnicity, language, nationality, country of birth and Early Years Pupil Premium (EYPP) eligibility etc.)
- Attendance information (such as sessions attended, number of absences and the reasons for the absence, occasions of lateness to session etc.).

Why we collect and use this information:

We use the child's data for the following reasons:

- to support the child's learning
- to assess/monitor and report on the child's progress
- to provide appropriate pastoral care
- to provide appropriate medical care for diagnosed conditions e.g. asthma, diabetes etc.
    - Please note that we will ask for your consent to administer prescription medication when there is a requirement to do so.
- to assess and identify children with Special Educational Needs and Disabilities (SEND)
- to assess the quality of our services
- to collaborate with external professionals to enhance the quality of teaching and learning in our schools
    - Please note that we will ask, as part of our induction processes, for your specific permission for your child to participate in all work that includes collaboration with our external professional partners.
- to comply with the law regarding data sharing.

The lawful basis on which we use this information:

As the data controller for the Federation, the Headteacher ensures that the Federation's practises adhere to the Data Protection Act 1998 and the General Data Protection Regulation (GDPR), which came into effect on 25 May 2018. Under Article 6 'Lawfulness of Processing' the processing shall be lawful if at least one of the specific purposes applies e.g. *(1c) processing is necessary for the compliance with a legal obligation to which the controller is subject'.*

Under Article 9 'Processing of Special Categories of Personal Data' the processing shall be lawful if e.g. *(2a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject'.*

Collecting a child's information:

Whilst the majority of children's information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing children's data:

Guidance for the Federation is obtained from the Records Management Society of Great Britain - Retention Guidelines for Schools Schedule, which is the recommended source for retention of records for all Wolverhampton Local Authority schools. The length of time for which we hold children's data varies e.g. Attendance Registers are retained from the date of the register + 3 years, although a child's SEN file/Individual Education Plan (IEP) etc. should be retained from the Date of Birth of the child for a period of 25 years, all documentation is transferred with the child to their Primary School, unless there is a robust reason for retention in school. Should you require further clarification please do not hesitate to speak to a member of the Senior Leadership Team (SLT).

Who we share children's information with

We routinely share children's information with:

- schools that the children attend after leaving us
- our Local Authority, which includes professionals from Speech and Language; Health Visitors etc.
- the Department for Education (DfE).

Why we share children's information:

We do not share information about our children with anyone without consent unless the law and our policies allow us to do so.

We share children's data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment, policy and monitoring.

We are required to share information about our children with our Local Authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (DfE) (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The National Pupil Database (NPD):

The NPD is owned and managed by the Department for Education (DfE) and contains information about all children, in schools, in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

Law requires us, to provide information about our children to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information.

The department may share information about our children from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance.

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data.

To be granted access to a child's information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data.

For information about which organisations the department has provided children's information to, (and for which project), please visit the following website: https://www.gov.uk/government/publications/national-pupil-database-requests-received.

To contact DfE: https://www.gov.uk/contact-dfe.

Requesting access to your personal data:

Under data protection legislation, parents and children have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Mrs Susan Lacey, Headteacher of Ashmore Park and Phoenix Nursery Schools Federation.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using your personal data, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact:

If you would like to discuss anything in this privacy notice, please contact:

Mrs Susan Lacey

Headteacher

Ashmore Park and Phoenix Nursery Schools Federation

Ashmore Park Nursery School

Griffiths Drive

Wolverhampton

WV11 2LH

Appendix 4: Personal data breach procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people.
- The DPO will alert the Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or Data Processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way); in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the individual School's computer system, in the GDPR file, in a sub-file entitled 'Data Breaches – Private and Confidential'.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned.
    - The name and contact details of the DPO

- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned.
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

  Records of all breaches will be stored on the individual School's computer system, in the GDPR file, in a sub-file entitled 'Data Breaches – Private and Confidential'.
- The DPO and Headteacher, Chair of Governors and all relevant Data Processors will meet to review what has happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the individual School's Local Authority ICT representative to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure that they receive a written response from all the individuals who received the data, confirming that they have complied with the request*

- *The DPO will carry out an internet search to check that the information has not been made public; if it has, they will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*
- *The Headteacher shall ensure that any document detailing staff pay information is anonymised prior to being shared with Governors.*