

Data Protection Policy and Toolkit - 2020

Rationale

Schools handle increasing amounts of personal information and have a statutory requirement to comply with **the EU General Data Protection Regulation (GDPR)** and any domestic data protection legislation (currently the Data Protection Act 2018). Together these will be referred to as “the Data Protection Legislation” in this note.

- Schools should have clear policies and procedures for dealing with personal information, and be registered with the Information Commissioner’s Office (ICO).
- Schools should have systems in place to reduce the chances of a loss of personal information, otherwise known as a data breach, which could occur as a result of theft, loss, accidental disclosure, equipment failure or hacking.
- On all occasions, any guidance from the ICO should be adhered to and incorporated into policies and procedures of the school.
- DCC accepts no responsibility for a school failing to comply with the Data Protection Legislation based on an interpretation of this template.

Data Protection – school policy

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents and pupils to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff and governors).

1.1. Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.

Keeping children safe in Education

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

1.2. It is a statutory requirement for all schools to have a Data Protection Policy:

<http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools>

In addition to this policy, schools should have:

- **Retention Information** - details on how long all records are retained (see audit)
- **Information Asset Audit** - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- **Privacy Notices** - for pupils, parents, staff and governors
- **Registered with the ICO**

This policy will link with the following:

- Safeguarding Policy
- Staff AUP/Code of Conduct
- Photographic Policy
- Photographic Consent Forms

1.3. Definitions

- Personal Data - information relating to a living individual, who can be identified directly from that data or indirectly by reference to other data held. (Note that information can be in any form - written, on a PC e.g. names, addresses, photos.)
- Data Processor – a person who handles the data including filing or storing it.
- Data Subject – the person about whom personal data is processed or kept.
- Data Controller - the person or organisation who determines the “how and what” of data processing in an organisation.

1.4. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) 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, subject to measures respecting the principle of ‘data minimisation’, not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) 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;
- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the ‘data minimisation’ principle; and

- f) 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.

In addition, Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

2. Lawful Basis for Processing Data

GDPR stipulates that there must be a lawful basis for processing data, and that for special category data an additional condition has to be met. The vast majority of information that schools collect and process is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority vested in the school, as the data controller. This is the main lawful basis for processing data that a school is likely to rely on.

There are other bases that may be available, such as a specific legal obligation applying to the data controller that makes the processing necessary. Your legal advisor will be able to identify individual statutes if required.

2.1 Age

Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians can do this on their behalf, providing this is in the best interests of the child. See <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/> Children should be provided with age appropriate advice about how their data is used (see *Personal Data for Pupils* guide).

2.2 Consent

If there is a lawful basis for collecting data, then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

3. RIGHTS

GDPR provides the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Different rights attach to different lawful bases of processing:

	Right to erasure	Right to portability	Right to object
Vital Interests	✓	X	X
Legal Obligation	X	X	X
Public Task	X	X	✓
Legitimate Interests	✓	X	✓
Contract	✓	✓	X
Consent	✓	✓	X but right to withdraw consent

3.1. The right to be informed – See *Privacy Notices section 6.2*

3.2. The right of access

Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

3.2.1. Subject Access request under GDPR

GDPR gives individuals the right to access any data that an organisation holds on them. Normally this has to be completed within 30 days without charge. Further guidance is available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/> Schools should be aware that guidance from the ICO highlights the rights of the child. *“Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident*

that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."

3.2.2. In maintained schools, parents have another statutory right to access their children's educational record

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 16 years and has to be completed in 15 working days. See <https://ico.org.uk/your-data-matters/schools/pupils-info/>

3.2.3. Information which may be withheld

On some occasions records could contain information which ***"is likely to cause significant harm to the physical or mental health of the child or others"***, for instance, if a child makes a disclosure of abuse. In these circumstances, the data should not be released and the pupil/parent does not need to be informed of its existence. If in doubt seek legal advice.

3.3. The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. Your legal advisor will be able to support with information about which data can continue to be legally held if a data subject asks to be 'forgotten'. Schools' data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that, where a school relies on either a 'legal obligation' or a 'public task' basis for processing (see above), there is no right to erasure – however, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or the school's data retention guidelines.

4. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

North Park Primary School 2020

The loss or theft of any Personal Data is a “Potential Data Breach”, which could result in legal action against the school. The loss of sensitive, or “special category”, personal data is considered much more seriously and the sanctions may well be more punitive.

4.1. Personal data

The school will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils-/students, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

4.2. Special Category Data

“Special Category Data” are data revealing a person’s racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person’s health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In a school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff (SEND)
- (some information regarding safeguarding will also fall into this category)
- staffing e.g. Staff Trade Union details.

Note – See section on Sharing Information.

4.3. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other ‘access to information’ procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources and other information about the school which does not relate to an individual. Some of this

data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school (if the school has written a detailed scheme of work that it wishes to sell to other schools). Schools may choose to protect some data in this category but there is no legal requirement to do so.

5. Responsibilities

The Headteacher and Governing Body are responsible for Data Protection; they should appoint a Data Protection Officer to manage data.

5.1. Risk Management – Roles: *Data Protection Officer*

The school should have a nominated member of staff responsible for the management of data protection.

Data Protection Lead - Mrs E Atkinson

According to the ICO the minimum role will include:

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

In some schools, other staff may have been delegated responsibility for particular issues, for instance the handling of SEND information.

5.2. Risk management - Staff and Governors Responsibilities

Everyone in the school has the responsibility of handling personal information in a safe and secure manner.

Governors 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 Governor.

Data Protection Governor – Mr N Foster

6. Legal Requirements

6.1. Registration

The school must be registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: <https://ico.org.uk/for->

[organisations/data-protection-fee](https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/) The register may be checked by visiting <https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/>

6.2. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents/carers of all pupils/students and staff of the data they collect, process and hold on the pupils/students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. More information about the suggested wording of privacy notices can be found on the DfE website:

<http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn>

Privacy notices should be made available to pupils, parents and carers, for instance, by publishing on the school website and making a paper copy available when children first register for school.

Children should be provided with age appropriate information about how their data is being used. (see *Personal Data for Pupils* guide).

7. Transporting, Storing and Disposing of personal Data

7.1. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

7.1.1. Technical Requirements

The school will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed)). Private equipment (ie owned by the users) must not be used for the storage of personal data.

The school/academy has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups. (Offsite backup managed by LA ITSS services; daily backups of servers)

7.1.2. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- the school will need to set its own policy as to whether data storage on removal media is allowed, even if encrypted – some organisations do not allow storage of personal data on removable devices
- *We would advise that...* Only encrypted removable storage purchased by the school is allowed to be used on school computers.

7.1.3. Passwords

All users will use strong passwords (Characters – ideally 14 - including a Capital letter, number and symbol) which must be updated occasionally. User passwords must never be shared. It is advisable NOT to record complete passwords, but prompts could be recorded.

7.1.4. Images

Images will be protected and stored in a secure area. See school Photographic Policy.

7.1.5. Cloud Based Storage

The school/academy has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by remote/cloud based data

services providers to protect the data. See advice from the DfE below:

<https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act>

7.2. Third Party data transfers

As a Data Controller, the school/academy is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party, as well as data processing agreements.

7.3. Retention of Data

The guidance given by the Information and Records Management Society – [Schools records management toolkit](#) can be used as a basis for determining how long records are kept. This school retention information should be available to data subjects on request.

Personal data that is no longer required will be destroyed and this process will be recorded.

7.4. Systems to protect data

7.4.1. Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- paper based safeguarding chronologies will be in a locked cupboard when not in use
- class lists used for the purpose of marking may be stored in a teacher’s bag.

Paper based personal information sent to parents (will be checked by ..., before the envelope is sealed).

7.4.2. School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

7.4.3. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

Where technically possible, all e-mail containing sensitive information will be encrypted by attaching documents that are password protected where the recipient will then need to contact the school for access to a one-off password

8. Data Sharing

8.1. Sharing with the LA and DfE

The school is required by law to share information with the LA and DfE. Further details are available at: <https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data>

8.2. Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children <https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Durham LSCB provides information on information sharing at: <http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf>

8.3. Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2018.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.
- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.
- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

9. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach, the data protection officer will inform the head teacher and chair of governors.
- When a personal data breach has occurred, the school must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then you must notify the ICO; if it's unlikely then you don't have to report it. However, if the school decide not to report the breach, they need to be able to justify this decision, and it should be documented.
- The school must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the school takes longer than this, they must give reasons for the delay.
- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Any report about a data breach must include:

- a description of the nature of the personal data breach including, where possible:
 - the categories and approximate number of individuals concerned;
and
 - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach;
and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

Further details are available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>

10. Policy Review Reviewing

This policy will be reviewed, and updated if necessary every two years or when legislation changes.

Date: 20.4.20

Review date

20.4.2022

Signed: *N Foster*
Chair of Governors

The Data Protection Officer is Mrs E Atkinson.

The Data Protection Governor is Mr Neil Foster.

Appendix 1 - Links to Resources and Guidance

ICO Guidance

Specific information for schools is available here. This includes links to guides from the DfE.

http://ico.org.uk/for_organisations/sector_guides/education

Specific Information about CCTV.

<https://ico.org.uk/media/1542/cctv-code-of-practice.pdf>

Information and Records Management Society – schools records management toolkit

A downloadable schedule for all records management in schools.

<http://irms.org.uk/page/SchoolsToolkit>

Disclosure and Barring Service (DBS)

Details of storage and access to DBS certificate information.

<https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information>

DFE

GDPR Toolkit

<https://www.gov.uk/government/publications/data-protection-toolkit-for-schools>

Privacy Notices

<https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices>

Use of Biometric Data

<https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools>

Safeguarding

<https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

and
<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>

Appendix 2 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR

All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:

The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR

The ICO website is here <http://ico.org.uk/>

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:

General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:

General information note from the Information Commissioner on publication of examination results.

Education Act 1996:

Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:

Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972:

Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:

Retention of school admission and exclusion appeal papers and other pupil records.

North Park Primary School Privacy notice for Parents/ Carers

This privacy notice explains how we collect, store and use personal data about pupils. We, North Park Primary School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Mrs Emma Atkinson.

Who we are and what we do

We are North Park Primary School, Bessmemer Green, Spennymoor, Co. Durham, DL16 6PP. We are a maintained primary school for children ages 3 – 11 years old. Our local authority is Durham County Council.

The personal data we collect and hold

We hold personal data about pupils, their parents or carers to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities, health care providers and the Department for Education.

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

- Contact details, contact preferences, date of birth, identification documents, National Insurance number.
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

Why we use this data

We use this data to:

- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of our services (including monitoring staff performance)

- Administer admissions waiting lists
- Carry out research
- Comply with the law regarding data sharing
- Identify pupil eligibility for Free School Meals and Pupil Premium funding

Our legal basis for using this data

We collect and use personal data on the basis of performing a public task (educating children).

On some occasions we may ask for consent to process data when its use is optional. On those occasions consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Collecting this information

We collect / obtain data from pupils, parents, carers, teachers and other professionals where relevant (e.g. G.P, hospital, social workers etc.)

How we store this data

We keep personal information about pupils, and their parents/guardians while they are attending our school. We may also keep it beyond their attendance at our school if this is necessary in order to comply with our legal obligations. We will only retain the data we collect for as long as is necessary. This would be to satisfy the purpose for which it has been collected in accordance with our data retention policy. Please contact us if you would like further details on this policy.

The security of data and information is important to us. This is why we follow a range of security policies and procedures to control and safeguard access to and use of your personal information. This includes both physical and technical security and integrity of all data.

Data sharing

We do not share any of this data with any other organisation without your permission, except where the law requires it. We are required to provide pupil data to central government through the Department for Education and the Education Funding Agency. Where it is necessary to protect a child, the school will also share data with the Local Authority Children's Social Services, medical professional and/or the Police.

We will share information with the local authority to check eligibility for free school meals.

We do not transfer personal data to countries outside the European Economic Area.

Parents and pupils' rights regarding personal data

Individuals have a right to make a '**subject access request**' to gain access to personal information that the school holds about them. This includes access to their child's educational record. This should be made in writing or by e-mail to northpark@durhamlearning.net The school will respond within a 15 school days timescale.

Parents/Carers can make a request with respect to their child's data where the child is not considered mature enough to understand their rights over their own data (usually under the age of 16), or where the child has provided consent.

Parents also have the right to make a subject access request with respect to any personal data the school holds about them.

If you make a subject access request, we will:

- Give you a copy of the information in an intelligible form
- Give you a description of the data we hold
- 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 or your child
- 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

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.

If we cannot provide information to you, we will give you a description of the information we hold and the reason why it cannot be disclosed to you at the time of your request.

Other rights

Individuals have rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

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.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contact us

North Park Primary School 2020

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

Mrs E Atkinson

Data Protection Officer

North Park Primary School

Bessemer Green

Spennymoor

County Durham

DL16 6PP

Tel: 01388815943

Sharing with the DfE and the Government

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

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

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the Department for Education and contains information about pupils 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. To find out more about the NPD, go to <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>

Sharing by the Department of Education

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

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

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: <https://www.gov.uk/government/publications/dfе-external-data-shares>

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

North Park Primary School Privacy notice for Staff

This privacy notice explains how we collect, store and use personal data about staff members. We, North Park Primary School, are the 'data controller' for the purposes of data protection law.

Our data protection officer is Mrs E Atkinson (deputy headteacher)

Who we are and what we do

We are North Park Primary School. We are a maintained primary school for children ages 3 – 11 years old. Our local authority is Durham County Council.

The personal data we collect and hold

We hold personal data about staff to support their employment and professional development, and to assess how the school is performing. We may also receive data about staff from previous employers, HR and occupational health workers.

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

- Contact details, contact preferences, date of birth, identification documents
- Professional development records
- Bank details
- Maternity/paternity pay information
- Health information
- Performance management documentation
- Characteristics, such as ethnic background, disability etc
- Sickness absence records
- Details of any professional support received
- Photographs/videos

Why we use this data

We use this data to:

- Support you in your professional roles
- Monitor and report on school improvement and self-evaluation
- Provide appropriate pastoral care
- Protect pupil welfare
- Ensure that the information we hold about you is kept up to date
- To share with agencies such as payroll and pensions

Our legal basis for using this data

We collect and use personal data on the basis of performing a public task (educating children).

On some occasions we may ask for consent to process data when its use is optional. On those occasions consent can be withdrawn at any time. We will make this clear when we ask for consent, and explain how consent can be withdrawn.

Collecting this information

We collect data from application forms, paper forms, online information, communication with yourself, information received from a third party (eg. referees, colleagues, agencies)

How we store this data

We keep personal information about staff while they are working at our school. We may also keep it beyond their time at our school if this is necessary in order to comply with our legal obligations.

We will only retain the data we collect for as long as is necessary. This would be to satisfy the purpose for which it has been collected in accordance with our data retention policy. Please contact us if you would like further details on this policy.

The security of data and information is important to us. This is why we follow a range of security policies and procedures to control and safeguard access to and use of your personal information. This includes both physical and technical security and integrity of all data.

Examples of our security include:

- Encryption, meaning that information is hidden so that it cannot be read without access knowledge (such as a password). This is done with a secret code or what's called a 'cypher'. The hidden information is said to then be 'encrypted';
- Controlling access to systems and networks allows us to stop people who are not allowed to view your personal information from getting access to it;
- Training for our staff allows us to make them aware of how to handle information and how and when to report when something goes wrong;
- Regular testing of our technology and ways of working including keeping up to date on the latest security updates (commonly called patches);

How long we keep your data for

This ranges from months for some records to decades for more sensitive records.

For example

- applications for recruitment will be kept for 1 year,
- your personnel record will be maintained for 25 years after you leave employment

Data sharing

North Park Primary School 2020

We may share your personal information where we have a statutory obligation to do so, such as for the purposes of the prevention or detection of crime, for legal proceedings, or where you have requested us to share information, such as childcare vouchers, pensions, mortgage applications etc.

Some examples of who we share information with include:-

- HMRC (Her Majesty's Revenue & Customs)
- DBS (Disclosure & Barring Service)
- Pensions schemes

If you would like confirmation of who we do share information with please contact us.

We do not process your personal information outside the EEC.

At no time will your information be passed to organisations external to us, or our partners for marketing or sales purposes, or for any other commercial use without your prior express consent.

Your information rights

Your Information Rights are set out in the law. Subject to some legal exceptions, you have the right to:

- Have any inaccuracies corrected;
- Have your personal data erased;
- Place a restriction on our processing of your data;
- Object to processing; and
- Request your data to be ported (data portability).

To learn more about these rights please see the ICO website.

To exercise any of these rights please contact the relevant service in the first instance.

You also have the right to request a copy of the personal information that the school holds about you. To do this, please ask the DPO (Mrs E Atkinson)

If something goes wrong with your personal information, or you have questions about how we use it, please contact Mrs E Atkinson (the Data Protection Officer)

If we have not been able to deal with your complaint, you can also contact the [Information Commissioner's Office](#)

Information Commissioner's Office
Wycliffe House,
Water Lane
Wilmslow, Cheshire SK9 5AF

Other rights

Individuals have rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)

North Park Primary School 2020

- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact our data protection officer.

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.

To make a complaint, please contact our data protection officer.

Alternatively, you can make a complaint to the Information Commissioner's Office:

- Report a concern online at <https://ico.org.uk/concerns/>
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

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:

Mrs E Atkinson

Data Protection Officer

North Park Primary School

Bessemer Green

Spennymoor

County Durham

DL16 6PP

Tel: 01388815943