Netherhall School
An Ambitious, Caring Community

GDPR Policy

Adopted by Netherhall School Governing Body

On: 20th August 2021

Signed:  (Fiona Woodward, Chair of Governors)

Date by which the procedure was last reviewed: 20th August 2021

Anticipated review date: 20th August 2022

Equality Act 2010
Our school is committed to equality both as an employer and a service provider. We welcome our general duty under the Equality Act 2010 to eliminate discrimination, advance equality of opportunity and foster good relations. In addition we recognise our specific duties to publish information every year about our school population; explain how we have due regard for equality; publish equality objectives which show how we plan to tackle particular inequalities and reduce or remove them.

We recognise our duty to ensure no-one experiences harassment, less favourable treatment or discrimination because of their age, any disability they may have, their ethnicity, colour or national origin, their gender identity or reassignment, their marital or civil partnership status, being pregnant or having recently had a baby, their religion or belief, their sexual identity and orientation.

We also welcome our duty under the Education and Inspections Act 2006 to promote community cohesion and British values.

Version No	Author/Owner	Date Written	Note of amendments made	Signature	Review Date
2018-01	AG/DS	April 2018	LA Policy sense checked		
2019-02	DS	May 2019			05/20
2020-21	DS/IAB	August 2021	Annual review	DS	08/21

Contents

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, 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.

Netherhall School follows Cumbria County Council's procedure with regard to the Privacy Notice which is issued to all new intake pupils and is published on the School's website. (See Appendix 1).

Schools are required to keep and process certain information about its pupils, staff and other individuals for various purposes such as:

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To ensure we operate efficiently and effectively;
- To recruit and pay staff;
- To collect fees;
- To comply with legal obligations to funding bodies and the government;
- To enable financial modelling and planning;
- To develop a comprehensive picture of the workforce and how it is deployed.

The school may be required to share personal information about its pupils or staff with other schools, organisations, the LA and social services.

This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage, biometric systems and audio and video systems.

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.

The Information Commissioner's Office (ICO) https://ico.org.uk/ gives further detailed guidance and the school undertakes to adopt and comply with ICO guidance.

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. This might include: • Employees (current and former), • Pupils (including former pupils), • Recruitment applicants (successful and unsuccessful), • Agency workers (current and former), • Casual workers (current and former), • Contract workers (current and former), • Volunteers (including members, directors and governors) and those on work placements, • Claimants.
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

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Netherhall School is registered as a data controller with the ICO and will renew this registration annually.

5. Roles and responsibilities

Our responsibilities as a data controller include:

- Analysing and documenting the types of personal data we hold and their uses.
- Identifying our lawful basis for processing personal data.
- Having procedures which support the rights of the individual.
- Ensuring consent procedures are lawful.
- Implementing and reviewing procedures to detect, report and investigate personal data breaches.
- Storing data in safe and secure ways.
- Assessing risks to individual rights and freedoms should data be compromised.

Staff responsibilities include:

- Understanding their data protection obligations in line with their training and professional duties.
- Checking that their data processing activities comply with our policy and are justified.
- Not using data in any unlawful way.
- Storing data carefully and correctly to avoid breaches of data protection.
- Raising concerns, notifying breaches or errors, and reporting anything suspicious or contradictory to this policy or our legal obligations without delay.

The Data Protection Officer's responsibilities include:

- Keeping governors updated about data protection responsibilities, risks and issues.
- Reviewing the data protection policy, associated policies and all relevant procedures regularly.
- Arranging data protection training and advice for all staff and others included in this policy.
- Advising on direct marketing issues such as compliance with the law and our policy; how we deal with queries from target audiences or media outlets; and the wording of data protection statements attached to emails and other marketing copy.
- Answering questions on data protection from staff, governors and other stakeholders.
- Responding to individuals such as parents, pupils and employees who want information.
- Checking on and approving of any third parties that handle our data and any contracts or agreements regarding data processing.

The Information Technology Manager's responsibilities include:

- Ensuring all systems, services, software and equipment meet acceptable security standards and can be appropriately filtered and monitored.
- Checking security hardware and software regularly to ensure it is functioning properly and securely.
- Researching relevant third-party services (cloud services, data shredding etc.) that we are considering using.

Our DPO is Jennifer Rowlands and is contactable via e-mail: Jennifer.rowlands@solway.cumbria.sch.uk or telephone: 07794 753 510

5.1 Headteacher

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

6. Data protection principles

In accordance with article 5 of the GDPR personal data will 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: ensuring that inaccurate personal data is erased or rectified without delay
- 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, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

This policy sets out how the school 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 school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the 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 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 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 pupil) 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.
Special categories of personal data can be lawfully processed under the following conditions:

a) Explicit consent of the individual, unless reliance on consent is prohibited by EU or Member State law.
b) 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.
c) Processing relates to personal data manifestly made public by the individual.
d) Carrying out obligations under employment, social security or social protection law, or a collective agreement.
e) Protecting the vital interests of an individual or another person where the individual is physically or legally incapable of giving consent.
f) The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
g) 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.
h) 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.

i) Reasons of public interest in the area of public health.

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

We collect and use workforce information for general purposes under paragraph 7.1c of this policy which complies with Articles 6 and 9 of the GDPR.

Under any other circumstances the legal basis for processing data will be identified and documented prior to data being processed.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

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 Local Authority's Records and Retention Policy.

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 pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. 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 pupils 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. Consent

It is not always necessary to gain consent before processing personal data but when it is, consent must be a positive indication.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.

A record will be kept documenting how and when consent was given.

If an individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then Netherhall School will ensure that the processing of that data does not take place.

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

Consent can be withdrawn by the individual at any time.

Parental consent will be sought prior to the processing of a child's data which would require consent until the age of 16, except where the processing is related to preventative or counselling services offered directly to a child.

Consent will be sought from the child after the age of 16 if we consider they have the competence to consent for themselves. If there is any doubt parental consent will continue to be required.

10. Subject access requests and other rights of individuals

10.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the school 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

To make a subject access request, please complete the subject access request form (Appendix 3), and return this 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 DPO.

10.2 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 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 pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

10.3 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 pupil 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 to be 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.

10.4 Other data protection rights of the individual

In addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it individuals also 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.

11. 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 pupil) within 15 school days of receipt of a written request.

12. Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils 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. The school 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 pupils 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 pupils. For example, pupils can pay for school dinners using a unique pin number required at each transaction if they wish.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil 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 pupil's parent(s)/carer(s).

Where staff members or other adults use the school's 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 the school will delete any relevant data already captured.

13. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. 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 Headteacher.

14. Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils 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 pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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.

15. 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 notices)
    - 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

16. Data security

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. All

members of Netherhall School are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party.

Physical measures

- Premises security measures, such as alarms and safes are in place. Gates surrounding school yards are locked during the day, and entrances onto site are locked during the night.
- Ensuring unauthorised personnel cannot see documents or screens which might display personal data e.g. open registers and visitor's books, emails, CCTV monitors.
- Only authorised persons are allowed in the IT Server room
- Disks, tapes and printouts are locked away securely when not in use.
- Visitors to schools are required to sign in and out, wear identification badges and are, when appropriate, accompanied.
- Premises security and storage systems are reviewed on a regular basis. If there is an increased risk in vandalism/theft, extra measures to secure data storage will be put in place.

Technical Measures

- Security software is installed on school networks. This includes internet filtering and firewall and antivirus.
- Data on network drives is password protected and automatically backed up off site. There are procedures in place to access and restore all the data held on the school network drives should this be necessary.
- Employees are given a secure user name and password to access the school network and other learning platform they require access to. These must not be disclosed to anyone or shared.
- 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 office and 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, the personal data must be kept secure at all times. The person taking the information off site must take full responsibility for data security.
- Staff must sign an acceptable use policy prior to being given access to the school network. This will be updated during the induction process.
- Electronic devices (such as staff computers) that are used to access personal data must be locked, even if left unattended for short periods
- Passwords containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as USB devices. Staff must not use USB devices unless they have been checked by IT to ensure they are encrypted. They must be password protected, stored in a secure and safe place when not in use, not accessed by other users (such as family members), data securely deleted when no longer required.
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment. Personal information should be saved on the school network and not on their own computer such as via their desktop.
- 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.

- Electronic devices (such as staff computers) that are used to access personal data must be locked, even if left unattended for short periods.
- E-mails containing personal data must be password protected/encrypted if they are being sent externally. Advice from the DPO must be sought if sending information outside the EU.
- Circular e-mails must be sent blind copy (bcc) to prevent e-mail addresses being disclosed to other recipients.
- Visitors must not be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- Personal data must not be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.

17. 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.

All confidential waste is removed safely from site by PW Confidential and disposed of safely and appropriately.

IT equipment is disposed of using PRM Green and data destruction certificates are provided. Please refer to the Disposal of IT Equipment policy.

18. Personal data breaches

The school 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 4.

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 pupils 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 pupils

19. Training

All staff and governors are provided with a copy of this policy, and must sign a declaration to accept that they have read and understood its content.

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

20. Monitoring arrangements

The DPO is 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) – if any changes are made to the bill that affect our school's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.

21. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Online Safety Policy
- Child protection and safeguarding policy
- CCTV Policy

APPENDIX 1

Privacy Notice (How we use pupil information)

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information(such as reports, feedback, test data and exam results)
- Relevant medical information (such as medication details, allergies, medical conditions and notes from meetings/GPs/other health care professionals)
- Post 16 learning information and destination data
- Special Educational needs information (such as ECHP's, Individual Health care plans and notes from review meetings and professional assessments)
- Exclusion and behaviour information
- Biometric information for the cashless catering system

Why we collect and use this information

We collect and use the pupil data for the following purposes:

- to support pupil learning
- to monitor and report on pupil attainment and progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to keep children safe (food allergies, emergency contact details)
- to meet statutory duties placed upon us for DFE data collections

The lawful basis on which we use this information

We collect and use pupil information under paragraph 7.1 which complies with Articles 6 and 9 of the GDPR.

Collecting pupil information

Whilst the majority of pupil 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 pupil information to us or if you have a choice in this. We may also receive information about pupils from other organisation's such as their previous school, local authority or the Department of Education.

Storing pupil data

The length of time we hold pupil information is set out in the Local Authority Records and Retention policy.

Who we share pupil information with

We routinely share pupil information with:

- schools that the pupil's attend after leaving us
- our local authority
- the Department for Education (DfE)
- School nurses
- Youth support services
- other public services that have a lawful right to collect pupil information
- third parties as listed in Appendix 5 of the GDPR policy.

Why we share pupil information

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

We share pupils' 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 pupils 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 (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Youth support services

Pupils aged 13+

Once our 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
- careers advisers

A parent or guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child/pupil once he/she reaches the age 16.

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
- careers advisers

For more information about services for young people, please visit our local authority website.

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.

We are required by law, to provide information about our pupils 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 pupils 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 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 pupil 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 pupil information, (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 pupils 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, please contact Netherhall School.

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/

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 school's computer system.
- 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 school's computer system
- The DPO and headteacher will meet to review what 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.

Sensitive information being disclosed via email (including safeguarding records)

- *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 ICT department 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 we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

APPENDIX 3

ACCESS TO PERSONAL DATA REQUEST
(Subject Access Request – SARS)

Enquirer's Surname		**Enquirer's Forenames**	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring:			
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please dispatch reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the school search its records based on the information supplied above under Section 7 (1) of the Data Protection Act 1998 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the school.

I agree that the reply period will commence when I have supplied sufficient information to enable the school to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Dispatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

Third Party Suppliers

- MLS (Library Software)
- School ICT Services (Cumbria County Council)
- CRB (Cashless Catering) [Including Biometric Data]
- Doddle
- Kerboodle
- MyMmaths
- ~~Sam learning~~ *(may retain data for a time period)*
- JED
- School fund manager
- Evolve
- Microsoft (Emails)
- Exam boards
- KT Tuition
- Supply agencies
- UCAS
- Renaissance Learning *(English Department)*
- ~~GL Assessment (CAT Tests)~~ *(may retain data for a time period)*
- Police
- Sports coaches
- FMS (Finance Software)
- CAPITA HR Solutions
- Capita (SIMS & SIMS Support)
- Work Experience companies
- Inspira
- PRM Green
- PW Confidential
- System IT
- Overnet Data - Edulink One
- Hegarty Maths
- Pearson Active Learn
- Microsoft Office – 365
- Microsoft Office Active Directory