Newlands CofE School Federation

Roots to grow… wings to fly

Data Protection Policy

Date adopted by governors: Spring 2022

Date for review: Spring 2023

STATUS: STATUTORY

REVIEW: ANNUALLY

COMMITTEE: RESOURCES

Data Protection Policy

Reviewed: Spring 2022 **Next Review: Spring 2023** **Committee: Resources** **Status: Statutory**

Contents

1. Aims

Newlands CofE School Federation comprises Shere CofE Infant School and Nursery and Clandon CofE Primary School. The Federation 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.

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.

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, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The Newlands Federation processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

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

5. Roles and responsibilities

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

5.1 Governing Body

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

5.2 Data protection officer

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

The DPO will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the Governing Body their advice and recommendations on data protection issues relating to either school.

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

The Federation's DPO is Sapphire Consulting and is contactable via DPO@shere.surrey.sch.uk.

5.3 Headteacher

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

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Federation of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
- If they have any concerns that this policy is not being followed
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

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

The principles say that personal data must be:

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

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the Federation can **fulfil a contract** with the individual, or the individual has asked the Federation to take specific steps before entering into a contract
- The data needs to be processed so that the Federation can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the Federation, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Federation 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.

If the Federation offers online services to pupils, such as classroom apps, and intends to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.2 Limitation, minimisation and accuracy

The Federation 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 the Federation wants 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 *Information and Records Management Society's toolkit for schools.*

8. Sharing personal data

The Federation 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

The Federation 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. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period

- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests should be submitted in writing, either by letter, email or fax 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.

9.2 Children and subject access requests

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

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at either of our schools may 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or voluminous. We will inform the individual of this within one 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.

9.4 Other data protection rights of the individual

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

10. Parental requests to see the educational record

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

11. Photographs and videos

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

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

Uses may include:
- Within either school on notice boards and in school brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school websites 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.

See our Child Protection and Safeguarding Policy/e-Safety Policy for more information on our use of photographs and videos.

12. 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 Federation'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 the Federation 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

13. Data security and storage of records

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

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on 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, staff must sign it in and out from the school offices
- Passwords that are at least 8 characters long 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 laptops and USB devices
- 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 (see our e-safety policy which includes an acceptable use agreement)
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

14. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the Federation's behalf. If we

do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

15. Personal data breaches

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

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

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 either of the schools' websites 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

16. Training

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

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

17. 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 the Federation's practice. Otherwise, or from then on, this policy will be reviewed **annually** and shared with the full Governing Body.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- E-safety policy

Appendix 1: 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 Federation'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 Federation'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 2: Data Protection Act 2018 – Subject Access Request

Dear Mr _____

Thank you for your request which we received on_____. Your request falls under the Data Protection Act 2018 as your request is for personal information concerning your child.

We do take the handling of personal data seriously and we ask you to please provide two proofs of ID such as a copy of your passport/birth certificate and a copy of proof of address such as a utility bill. This is to ensure that we are sending personal data to the right individual.

In order for us to process your request efficiently, it would be most helpful if you can specify the date range that you require information for and any particular information that you require. As you can understand there is a large amount of information held and we wish to ensure that you are supplied with the relevant information.

On receipt of the above ID, we will process your request within the one month statutory reply period.

Yours sincerely

Dear

RE: YOUR REQUEST UNDER THE DATA PROTECTION ACT 2018

Thank you for your subject access request dated XXXX. Subject access requests are for personal data about the requester that is focused on the requester. It is for data/information and not the documents in which the data/information is found.

You have been quite specific in your request, which was for the following information held by the school:

STATE REQUEST

We searched our relevant systems to locate data within the scope of your request. The data retrieved was reviewed by the Senior Management to ensure it was your personal data.

- I confirm that we are processing the personal data specified in your request.

I enclose with this letter a copy of the document/s specified in your request.

We have redacted any reference to third parties where applicable and where we owe a duty of confidentiality.

I hope that the information attached satisfies your request.

If you are unhappy with the contents of the information provided, its accuracy or retention, or with the handling of your request, then you should raise this by writing to the Chair of Governors.

If, following this, you are not satisfied by the Newlands CofE School Federation's response to your complaint, you have the right to apply to the Information Commissioner for a decision. The Information Commissioner will normally expect you to have exhausted our complaints procedure. The Information Commissioner can be contacted at the Cheshire address below.

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

We supply this information based on your original request. Please do not hesitate to contact me at the above address, should you have any queries regarding the information enclosed.

Yours sincerely

Headteacher
Newlands CofE School Federation

Appendix 3: Fair Processing Notice

Newlands CofE School Federation collects data and information about our pupils and their parents/ carers/ guardians so that we can run our schools effectively and comply with our duties and obligations. This Fair Processing Notice explains what data we process, why we process it, our legal basis, how long we keep it and the rights of our pupils and their parents, carers or guardians.

We will always make sure that our pupils' information is protected and treated securely. Any information that we process will be held in accordance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 and other UK or EU data protection legislation.

Our contact details

Shere CofE Infant School and Nursery **Gomshall Lane** **Shere** **Guildford** **Surrey** **GU6 8JP**	**Clandon CofE Primary School** **The Street** **West Clandon** **Surrey** **GU4 7ST**
01483 202198	**01483 222442**
info@shere.surrey.sch.uk	**info@clandon.surrey.sch.uk**

Our Data Protection Officer is Kristy Gouldsmith and can be contacted at **dpo@shere.surrey.sch.uk.**

What pupil data is processed?
The pupil record starts its life when a file is opened for each new pupil as they begin school. This is the file which will follow the pupil for the rest of his/her school career. If a child transfers to either of our schools, their file will also be sent to the relevant school.

The file contains the following data, as applicable to the child:

- Surname
- Forename
- DOB
- Unique Pupil Number
- The name of the pupil's doctor
- Emergency contact details
- Gender
- Preferred name
- Position in family
- Ethnic origin
- Language of home (if other than English)
- Religion
- Names of adults who hold parental responsibility with home address and telephone number (and any additional relevant carers and their relationship to the child)
- Name of the school, admission number and the date of admission and the date of leaving.
- Any other agency involvement e.g. speech and language therapist, paediatrician
- The record of transfer from previous school
- Any information regarding free school meals
- Dietary requirements
- Any information relating to a major incident involving the child (either an accident or other incident)
- Any reports written about the child
- Any information about a statement and support offered in relation to the statement

- Child protection reports/disclosures
- Safeguarding information (such as court orders and professional involvement)
- Special educational needs (including the needs and ranking)
- Medical and administration (such as doctor's information, child health, dental health, allergies, medication and dietary requirements)
- Attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- Assessment and attainment
- Behavioural information (such as exclusions and any relevant alternative provision put in place)
- Any information relating to exclusions (fixed or permanent)
- Any correspondence with parents or outside agencies relating to major issues
- Details of any complaints made by the parents or the pupil
- Absence notes
- Parental consent forms for trips/outings (in the event of a major incident all the parental consent forms will be retained with the incident report not in the pupil record)
- Forms relating to any clubs
- Correspondence with parents about minor issues
- Accident forms
- Image related to identify management/authentication

We will also hold data about pupils that we have received from other organisations, including other schools, local authorities and the Department for Education.

What parent data is processed?

- Surname
- Forename
- Contact details
- Any correspondence with parents or outside agencies relating to major or minor issues
- Details of any complaints made by the parents or the pupil
- Parental consent forms for trips/outings (in the event of a major incident all the parental consent forms will be retained with the incident report not in the pupil record)
- Consent forms for clubs
- Image when visiting the school

How is pupil and parent data collected?

We collect pupil information via:

- you directly
- external agencies, such as Local Council, Department of Education, etc.

Pupil and parent data are essential for the schools' operational use. Whilst the majority of information that you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

Why is pupil data being collected and how will it be used?

The personal data of the pupil and the parent is required for the pupil to attend one of our schools, to best meet the needs of the pupil whilst attending that school and for communications between us and you.

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
- Administer admissions waiting lists

- Carry out research
- Comply with the law regarding data sharing
- Keep pupils safe
- To meet the statutory duties placed upon us for DfE data collections and for the Local Authority data collections

Legal basis
We only collect and use the pupils' personal data when the law allows us to. Most commonly, we process it where:

- We need to comply with a legal obligation
- We need it to perform an official task in the public interest

Public Interest	Providing an education. Fulfilling the safeguarding and special educational needs obligations for our pupils.
Legal Obligation	Details are used for statutory reporting requirements to the Department of Education, local council and third parties such as courts or police where we are legally obliged to do so. We will also process personal data and share it with outside agencies in safeguarding situations.
Vital Interests	Pupil details may be required, such as allergy information, for their own protection and wellbeing.
Contract	Pupil details are required to satisfy a contract for any fees (e.g. clubs, trips, lunches etc)
Legitimate interest	Parent details are used to communicate events and activities that are part of the Federation's ethos. We use a variety of different software in our schools. Technology allows us to provide an enriched learning environment and to best record information about our students. CCTV for security, safety and crime prevention.
Consent	If you wish for your child to take part in any church activities, we will ask for your consent to share your child's data with the church.

Some of the reasons listed above for collecting and using pupils' personal data overlap and there may be several grounds which justify our use of this data.

Who will it be shared with?
Personal data of pupils will be shared with:

Local Council	Personal data will be shared with the local council for purpose of education provision and performance monitoring.
Department of Education	Personal data will be shared into the National Pupil Database, owned by the DfE, for the purpose of school funding, educational attainment policy and monitoring. For completing census returns.
Contractors	Personal data may be passed to contractors for providing extra activities or clubs or meal provisions.
School Staff	Personal data will be shared with appropriate members of staff for the purpose of pupil welfare, such as, understanding medical needs.
Health Providers	Personal details will be shared with immunisation and statutory pupil health monitoring services, school nurse, NHS

External Education Resources	Personal details maybe shared with external education resources to allow pupils access to extra resources
SENCO Specialists	Personal data may be passed to specialists involved with the SENCO provision for the pupil.
Service Providers	Personal data will be shared with our service providers, such as software platforms.

Department for Education
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

- Pupil transfer forms
- School census

School census
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under Section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

How the Government uses your data
The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of pupils 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
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 pupils 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 one 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/dfe-external-data-shares

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

Local Authority

We may be required to share information about our pupils with the local authority to ensure that they can conduct their statutory duties, for example, under the Schools Admission Code, including conducting Fair Access Panels.

How we store your data
Personal data is stored in accordance with our Data Retention Policy.

How long do we keep your personal data
We hold pupil data securely while they are attending either of our schools. We may also keep it beyond their attendance at the relevant school if this is necessary in order to comply with our legal obligations. We retain personal data in accordance with our Data Retention Policy.

Transferring data internationally
While we make every effort to ensure that data is kept in the EU or EEA, some of our software providers may host the data in countries outside of the EU or EEA. Please enquire if you wish to have this information.

What are your privacy rights
Under GDPR, 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, contact our DPO.

Depending on the lawful basis above, you may 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
- a right to seek redress, either through the ICO, or through the courts
-

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

For more information about your Data Subject Rights, please refer to the ICO website – https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulations-gdpr/individual-rights/

We are registered with the Information Commissioner's Office.

Contact
If you would like to discuss anything in this privacy notice, please contact our DPO.