St John and St Nicolas Schools Federation

For the good of all through curiosity, creativity and love

Policy Title:	**Data Protection Policy**
Policy Reference:	**SJN021**
Description:	Processes for collection, storage and use of personal data
Status:	Approved by Governing Board
Category:	Statutory
Review frequency:	Every two years
Contact:	governors@stjohnandstnicolasschools.org.uk
Version:	**V1.2**
Other relevant policies:	Child Protection, E-Safety, Freedom of Information
Date for Review:	February 2028

Change Record				
Version Number	**Date Approved**	**Governing Board Minute Reference**	**Description of Amendments**	**Review Date**
1.0	*06.12.21*	*FGB Minutes 06.12.21*	*Prepared by executive headteacher and ratified by FGB*	*Dec 2023*
1.1	*04.12.23*	*FGB Minutes 04.12.23*	*No amendments identified; ratified by FGB*	*Dec 2025*
1.2	*23.6.26* *14.7.26*	*S&C Minutes 23.6.26* *FGB Minutes 14.7.26*	*Update version number, index page numbers and WBC Data Protection Officer*	*Feb 2028*
1.3				
1.4				

Index		Page
1.	Aims	3
2.	Legislation & Guidance	3
3.	Definitions	3
4.	The Data Controller	4
5.	Roles & Responsibilities	4
6.	Data Protection Principles	5
7.	Collecting Personal Data	5
8.	Systems and Storage	6
9.	Data Sharing	6
10.	Internal Responsibilities	6
11.	Sharing Personal Data	7
12.	Subject Access Requests and other Rights of Individuals	7
13.	Parental requests to see Educational Record	9
14.	Photographs & Videos	9
15.	Data Protection by Design & Default	10
16.	Data Security & Storage of Records	10
17.	Data Security in Practice	11
18.	Disposal of Records	11
19.	Personal Data Breaches	11
20.	Training	11
21.	Monitoring Arrangements	12
22.	Links with Other Policies	12
	Appendix 1 – Personal Data Breach Procedure	12
	Appendix 2 – Model Privacy Notices	14

St John and St Nicolas Schools Federation Data Protection Policy

At St John and St Nicolas Schools Federation, our vision is 'For the good of all – through curiosity, creativity and love.' This vision inspires everything that the federation does. It applies equally to all the federation's policies with the intention that our policies impact as fairly and positively as possible to meet the needs of all members of our schools' community.

1. Aims

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 & 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. In addition, this policy complies with the federation's funding agreement and articles of association.

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
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 • 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.

Data subject	Processing can be automated or manual. The identified or identifiable individual whose personal data is held or processed.
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 federation's schools process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

Both schools are registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles & Responsibilities

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

Governing Board

The governing board has overall responsibility for ensuring that the federation complies with all relevant data protection obligations.

Data Protection Officer (DPO)

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring the federation's compliance with data protection law, and developing related policies and guidelines where applicable.

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

The DPO is also the first point of contact for individuals whose data the federation processes, and for the ICO. Full details of the DPO's responsibilities are set out in their job description (West Berkshire Council SLA).

The DPO's contact details are below:
West Berkshire Council Data Protection Officer
Gerard Strong
West Berkshire Council
Market Street, Newbury
Berkshire RG14 5LD
Email: dp@westberks.gov.uk
Telephone: 01635 551111 (WBC switchboard)

Headteacher
The executive headteacher and heads of school acts as the representative of the data controller on a day-to-day basis.

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 United Kingdom.
    - 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 fulfill 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 our federation aims to comply with these principles.

7. Collecting Personal Data

a. Lawfulness, fairness and transparency

The federation will only process personal data where it has 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 **fulfill 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, the federation 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 intend to rely on consent as a basis for processing, they will get parental consent (except for online counselling and preventive services).

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

b. Limitation, minimisation and accuracy

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

If they want to use personal data for reasons other than those given when they first obtained it, they will inform the individuals concerned before they 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. Systems and Storage

The federation primarily stores and processes personal data using SIMS for overall data management, CPOMS for safeguarding and behaviour management and secure Microsoft 365 systems including email and SharePoint.

9. Data Sharing

The federation routinely shares data with the local authority, safeguarding partners, the Department for Education and approved third-party providers including SIMS and Ask4Support (IT support). Third-party data is also shared securely with key partners through the Wonde platform. These include West Berkshire, Department for Education, Developing Experts (curriculum provider), FFT (curriculum provider), Get Set for Education (curriculum provider), Insight Tracking (data analysis platform), Primary Site (website provider).

10. Internal Responsibilities

The Executive Headteacher oversees compliance on a day-to-day basis, supported by the school office, who manage record keeping, data requests and communication with external agencies.

11. 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 staff at risk
- They need to liaise with other agencies – they will seek consent as necessary before doing this
- The suppliers or contractors need data to enable the federation to provide services to its staff and pupils – for example, IT companies. When doing this, the federation 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 the federation shares
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the federation.

The federation will also share personal data with law enforcement and government bodies where they 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 their safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

The federation may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of its pupils or staff.

Where the federation transfers personal data to a country or territory outside the United Kingdom, they will do so in accordance with data protection law.

12. Subject Access Requests and other Rights of Individuals

a. 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 must be submitted in writing, by email or letter to the school office. 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.

b. 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 (Primary School):

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 the federation's 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.

c. Responding to subject access requests

When responding to requests, the federation:

- 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. They will inform the individual of this within 1 month, and explain why the extension is necessary.

The federation 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, the federation 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 the federation refuses a request, they will tell the individual why, and tell them they have the right to complain to the ICO.

d. 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 the federation are collecting their data about how they use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask the federation 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 United Kingdom
- 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.

13. Parental requests to see Educational Record

The federation's policy is that they give the right for parental access 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.

14. Photographs & Videos

As part of school activities, the federation may take photographs and record images of individuals within either of the schools.

Pupils aged under 18 years of age

The federation will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

They will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where they don't need parental consent, they will clearly explain to the pupil how the photograph and/or video will be used.

Uses may include:

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

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

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

See the federation's Child Protection and Safeguarding Policy for more information on the federation's use of photographs and videos.

15. Data Protection by Design & Default

The federation will put measures in place to show that they have integrated data protection into all of their 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; they will also keep a record of attendance
- Regularly conducting reviews and audits to test their privacy measures and make sure they are compliant.

Maintaining records of their processing activities, including:

- For the benefit of data subjects, making available the name and contact details of both schools and DPO and all information they are required to share about how they use and process their personal data (via the federation's privacy notices)
- For all personal data that they hold, maintaining an internal record of the type of data, data subject, how and why they are using the data, any third-party recipients, how and why they are storing the data, retention periods and how they are keeping the data secure.

16. Data Security & Storage of Records

The federation 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 relevant school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. 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 where personal information is stored
- 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 the federation's E-Safety policy on acceptable use)
- Where they need to share personal data with a third party, they carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

17. Data Security in Practice

All staff access school systems through password protected accounts. Access to sensitive systems is role-based and reviewed periodically. Paper records are stored in locked cabinets within secure areas of the school.

18. 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 they cannot or do not need to rectify or update it.

For example, they will shred or incinerate paper-based records, and overwrite or delete electronic files.

They may also use a third party to safely dispose of records on the federation's behalf. If they do so, they will require the third party to provide sufficient guarantees that it complies with data protection law.

19. 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, they will follow the procedure set out in Appendix 1.

When appropriate, they 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 federation's 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.

20. 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.

21. Monitoring Arrangements

The governing board is responsible for monitoring and reviewing this policy.

22. Links with Other Policies

This data protection policy is linked to other policies including:

- Freedom of information policy (including publication scheme)

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 executive headteacher, who will liaise with the Data Protection Officer. The school maintains a breach log and follows the agreed reporting procedure.
- 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 executive 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 by the DPO on the Federation's central systems.

- 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 by the DPO on the federation's central systems.
- The DPO and executive 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
The federation 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. They 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 the federation receives 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, the federation will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted Other types of breach that the federation might want to consider could include:
- Details of pupil premium interventions for named children being published on the federation's website
- Non-anonymised pupil exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- Either school's cashless payment provider being hacked and parents' financial details stolen

Appendix 2 – Model Privacy Notices

1. Privacy notice for parents/carers

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

This privacy notice explains how they collect, store and use personal data about **pupils**.
The federation is the 'data controller' for the purposes of data protection law.

The federation's data protection officer and contact details are below (see 'Contact us' below).

The personal data the federation holds

Personal data that they may collect, use, store and share (when appropriate) about pupils includes, but is not restricted to:
- Contact details, contact preferences, date of birth, identification documents
- Results of internal assessments and externally set tests
- Pupil and curricular records
- Characteristics, such as ethnic background, eligibility for free school meals, or special educational needs
- Exclusion information
- Details of any medical conditions, including physical and mental health
- Attendance information
- Safeguarding information
- Details of any support received, including care packages, plans and support providers
- Photographs

They may also hold data about pupils that they have received from other organisations, including other schools, local authorities and the Department for Education.

Why they use this data
They use this data to:
- Support pupil learning
- Monitor and report on pupil progress
- Provide appropriate pastoral care
- Protect pupil welfare
- Assess the quality of their services
- Administer admissions waiting lists
- Comply with the law regarding data sharing

Their legal basis for using this data
They only collect and use pupils' personal data when the law allows them to. Most commonly, they process it where:
- They need to comply with a legal obligation
- They need it to perform an official task in the public interest

Less commonly, they may also process pupils' personal data in situations where:
- They have obtained consent to use it in a certain way
- They need to protect the individual's vital interests (or someone else's interests)

Where they have obtained consent to use pupils' personal data, this consent can be withdrawn at any time. They will make this clear when they ask for consent, and explain how consent can be withdrawn.

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

Collecting this information
While the majority of information the federation collects about pupils is mandatory, there is some information that can be provided voluntarily.

Whenever they seek to collect information from you or your child, they make it clear whether providing it is mandatory or optional. If it is mandatory, they will explain the possible consequences of not complying.

How they store this data
They keep personal information about pupils while they are attending the federation's schools. They may also keep it beyond their attendance at the schools if this is necessary in order to comply with their legal obligations.

Please refer to the Information and Records Management Society's toolkit for schools.

Data sharing
The federation does not share information about pupils with any third party without consent unless the law and the federation's policies allow them to do so.

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

- The local authority – to meet their legal obligations to share certain information with it, such as safeguarding concerns and exclusions
- The Department for Education
- The pupil's family and representatives
- Educators and examining bodies
- Their regulator [specify as appropriate, e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service the federation has contracted them for
- Financial organisations
- Central and local government
- Their auditors
- Survey and research organisations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies

National Pupil Database
They are required to provide information about pupils to the Department for Education as part of statutory data collections such as the school and early years census if applicable.

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

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

The Department for Education may share information from the NPD with other organisations which promote children's education or wellbeing in England. Such organisations must agree to strict terms and conditions about how they will use the data. For more information, see the Department's webpage on how it collects and shares research data. You can also contact the Department for Education with any further questions about the NPD.

Transferring data internationally
Where they transfer personal data to a country or territory outside the United Kingdom, they will do so in accordance with data protection law.

Parents and pupils' rights regarding personal data
Individuals have a right to make a **'subject access request'** to gain access to personal information that the federation holds about them.

Parents/carers can make a request with respect to their child's data where the child is not

considered mature enough to understand their rights over their own data (usually under the age of 12), or where the child has provided consent.

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

If you make a subject access request, and if they do hold information about you or your child, they will:

- Give you a description of it
- Tell you why they are holding and processing it, and how long they will keep it for
- Explain where they got it from, if not from you or your child
- Tell you who it has been, or will be, shared with
- Let you know whether any automated decision-making is being applied to the data, and any consequences of this
- Give you a copy of the information in an intelligible form

Individuals also have the right for their personal information to be transmitted electronically to another organisation in certain circumstances.
If you would like to make a request please contact the data protection officer.

Other rights

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

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

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

Complaints

The federation take any complaints about their collection and use of personal information very seriously. If you think that their collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about their data processing, please raise this with them in the first instance.

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

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

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

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

West Berkshire Council Data Protection Officer
Gerard Strong
West Berkshire Council
Market Street
Newbury
Berkshire RG14 5LD
Email: dp@westberks.gov.uk
Telephone: 01635 551111 (WBC Switchboard)

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way the federation use data in either of their schools.

2. Privacy notice for staff
Under data protection law, individuals have a right to be informed about how the federation uses any personal data that they hold about them. They comply with this right by providing 'privacy notices' (sometimes called 'fair processing notices') to individuals where they are processing their personal data.

This privacy notice explains how they collect, store and use personal data about individuals they employ, or otherwise engage, to work at either school.

The federation is the 'data controller' for the purposes of data protection law.

Their data protection officer is listed below (see 'Contact us' below).

The personal data they hold
They process data relating to those they employ, or otherwise engage, to work at their schools. Personal data that they may collect, use, store and share (when appropriate) about you includes, but is not restricted to:

- Contact details
- Date of birth, marital status and gender
- Next of kin and emergency contact numbers
- Salary, annual leave, pension and benefits information
- Bank account details, payroll records, National Insurance number and tax status information
- Recruitment information, including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process
- Qualifications and employment records, including work history, job titles, working hours, training records and professional memberships
- Performance information
- Outcomes of any disciplinary and/or grievance procedures
- Absence data

- Copy of driving licence
- Photographs
- Data about your use of the school's information and communications system

They may also collect, store and use information about you that falls into "special categories" of more sensitive personal data. This includes information about (where applicable):

- Race, ethnicity, religious beliefs, sexual orientation and political opinions
- Trade union membership
- Health, including any medical conditions, and sickness records

Why they use this data

The purpose of processing this data is to help them run the schools, including to:

- Enable you to be paid
- Facilitate safe recruitment, as part of their safeguarding obligations towards pupils
- Support effective performance management
- Inform their recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Improve the management of workforce data across the sector
- Support the work of the School Teachers' Review Body

Their lawful basis for using this data

They only collect, and use personal information about you when the law allows them to. Most commonly, they use it where they need to:

- Fulfill a contract they have entered into with you
- Comply with a legal obligation
- Carry out a task in the public interest

Less commonly, they may also use personal information about you where:

- You have given them consent to use it in a certain way
- They need to protect your vital interests (or someone else's interests)
- They have legitimate interests in processing the data

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

Some of the reasons listed above for collecting and using personal information about you overlap, and there may be several grounds, which justify the federation's use of your data.

Collecting this information

While the majority of information they collect from you is mandatory, there is some information that you can choose whether or not to provide to them.

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

How they store this data
They create and maintain an employment file for each staff member. The information contained in this file is kept secure and is only used for purposes directly relevant to your employment.

Once your employment with the federation has ended, we will retain this file and delete the information in it in accordance with the Information and Records Management Society's toolkit for schools.

Data sharing
They do not share information about you with any third party without your consent unless the law and their policies allow them to do so.

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

- Their local authority – to meet their legal obligations to share certain information with it, such as safeguarding concerns and [maintained schools only] information about Head Teacher performance and staff dismissals
- The Department for Education
- Your family or representatives
- Educators and examining bodies
- Their regulator [specify as appropriate e.g. Ofsted, Independent Schools Inspectorate]
- Suppliers and service providers – to enable them to provide the service the federation has contracted them for, such as payroll
- Financial organisations
- Central and local government
- Their auditors
- Survey and research organisations
- Trade unions and associations
- Health authorities
- Security organisations
- Health and social welfare organisations
- Professional advisers and consultants
- Charities and voluntary organisations
- Police forces, courts, tribunals
- Professional bodies
- Employment and recruitment agencies

Transferring data internationally
Where the federation transfer personal data to a country or territory outside the United Kingdom they will do so in accordance with data protection law.

Your rights
a. How to access personal information they hold about you
Individuals have a right to make a **'subject access request'** to gain access to personal information that the federation holds about them.

If you make a subject access request, and if they do hold information about you, they will:

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

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

If you would like to make a request, please contact the data protection officer.

b. Your other rights regarding your data
Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe. You have the right to:
- Object to the use of your personal data if it would cause, or is causing, damage or distress
- Prevent your data being used to send direct marketing
- Object to the use of your personal data for decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

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

Complaints
The federation take any complaints about their collection and use of personal information very seriously.

If you think that their collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about their data processing, please raise this with them in the first instance.

To make a complaint, please contact the data protection officer.
Alternatively, you can make a complaint to the Information Commissioner's Office:
- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113
- Or write to: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Contacting the Federation
If you have any questions, concerns or would like more information about anything mentioned in this privacy notice, please contact their **Data Protection Officer (DPO)**:
West Berkshire Council Data Protection Officer
Gerard Strong
School Improvement Advisor
West Berkshire Council

Market Street
Newbury, Berkshire RG14 5LD
Email: dp@westberks.gov.uk
Telephone: 01635 551111 (WBC Switchboard)

This notice is based on the Department for Education's model privacy notice for pupils, amended for parents and to reflect the way they use data in this federation.