Federation of Savile Town CE (C) and Thornhill Lees CE (VC) Infant & Nursery Schools

Data Protection Policy

Ratified On : January 2025

Review Date: January 2027

Contents

1. Aims and Intent

Federation of Savile Town CE (C) and Thornhill Lees CE (VC) 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 UK General Data Protection Regulation (UK-GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

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

The Federation is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK General Data Protection Regulation (UK GDPR).

The school may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the schools complies with the following core principles of the UK GDPR.

Organisational methods for keeping data secure are imperative, and Federation of Savile Town CE (C) and Thornhill Lees CE (VC) Infant & Nursery Schools believes that it is good practice to keep clear practical policies, backed up by written procedures.

2. Legislation and guidance

This policy meets the requirements of the UK-GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK-GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. Also, see our CCTV Policy.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.

Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

Our schools process 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 our Schools, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Board of Governors

The board has overall responsibility for ensuring that our Schools complies with all relevant data protection obligations.

5.2 Data Protection Officer

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

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

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

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

Our DPO is Matthew Keeffe of Keeffe and Associates Ltd and is contactable via email office@thornhilllees.com or via telephone on 01924 430548.

5.3 Head teacher

The Head teacher 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 School 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 of the United Kingdom and 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 UK GDPR is based on data protection principles that our School must comply with.

The principles say that personal data must be:

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

- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1 Lawfulness, fairness, and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g., to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carers 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 UK GDPR and Data Protection Act 2018.

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

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

7.2 Limitation, minimisation, and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain

these reasons to the individuals when we first collect their data.

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

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

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's Record Management and Retention Policy.

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to consult 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 conduct their service, and information necessary to keep them safe while working with us

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

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

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

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

9. Other rights of individuals

9.1 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 to or outside of the UK or European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, which 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 school activities, we may take photographs and record images of individuals within our School.

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/carers and pupil.

Uses may include:

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

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

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

See our safeguarding 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 school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to evaluate our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

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 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
- 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 acceptable use policy)
- Where we need to share personal data with a third party, we conduct due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)

NB: Also, see our Records Management and Retention Policy.

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

15. 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 school's processes make it necessary.

16. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated if a fundamental change in legislation occurs, otherwise this policy will be reviewed **every 2 years** and shared with the full governing board.

17. Personal data breaches

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

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

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

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

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, Business Manager and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material, or non-material damage (e.g., emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way) in case it is challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored on the school's computer system.
- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks, or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

- Facts and cause
- Effects
- Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored on the school's computer system.

- The DPO and Principal 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 Sender 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 Sender will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request and advise the DPO of the fact*
- *The ICT representative or DPO will conduct 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*

***Other types of breach that you might want to consider could include**:*

- *Details of pupil premium interventions for named children being published on the school 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*
- *The school's parent payment provider being hacked, and parents' financial details stolen*

Consequences of Failing to Report a Breach

Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of your global turnover. The fine can be combined the ICO's other corrective powers under Article 58, a sample of which are as follows:

a) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Regulation;
b) to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation;
d) to order the controller or processor to bring processing operations into compliance with the provisions of this Regulation, where appropriate, in a specified manner and within a specified period;
e) to order the controller to communicate a personal data breach to the data subject;
f) to impose a temporary or definitive limitation including a ban on processing;

NB: This list is not exhaustive

So, it is important that staff follow the breach-reporting process in place within this policy and to ensure we recognise, detect via our IT Team, and can notify a breach, on time; and to provide the necessary details. We shall use the ICO breach reporting form for this purpose as follows https://ico.org.uk/media/for-organisations/documents/2614197/personal-data-breach-report-form-web-20190124.doc .

It is imperative that, where staff feel a breach has occurred, they report this to the DPO, Head teacher or School Business Manager via **Annex A** or the Information Security Incident Report Form for electronic data contained in schools Retention policy at the earliest opportunity.

18. Links with other policies

This data protection policy is linked to our:

- Freedom of information Policy
- Freedom of Information Publication Scheme
- ICT Acceptable Use Policy
- Safeguarding Policy
- Safer Recruitment Practice

This policy will be reviewed on a bi-annual basis.

Annex A – Staff Internal Breach Report Form

Data Breach Report Form		
This form should be completed as soon as a data breach has been discovered. Please complete sections 1 -7 with as much information as possible and pass the form on to the DPO immediately. The breach will be recorded on the School's Breach Register and the Head teacher informed so that an investigation can be conducted		
	Report by:	
	Date	
1	**Nature of breach e.g., theft/disclosed in error/technical problem**	
2	**Description of how breach occurred:**	
3	**When was the breach reported and how did you become aware?**	
4	**Full description of all personal data involved**	
5	**Number of individuals affected?** **Have all individuals affected been informed**	
6	**What immediate remedial action was taken:**	
7	**Has the data been retrieved or deleted? If yes – date and time:**	
8	**Any Procedure changes needed to reduce risks of future data loss**	

9	**Conclusion**	

NB: Please return this form to the Head Teacher, School Business Manager or our DPO.

Annex B – Subject Access Request Process

Introduction
All personal data processed by Federation of Savile Town CE (C) and Thornhill Lees CE (VC) is within the scope of this policy. Personal data that is asked for as a matter of routine e.g., copies of employment contracts, job descriptions or other information already received by data subjects.

Data subjects are entitled to ask:
• Whether The Federation is processing any personal data about that individual and, if so, to be given:
- a description of the personal data;
- the purposes for which it is being processed; and,
- details of who will be allowed to see the personal data.

• To be given a copy of the information and to be told about the sources from which The Federation derived the information; and

Responsibilities
The Head teacher is responsible for the application and effective working of this policy and procedure, and for reporting to the Board of Governors on Subject Access Requests (SARs).

The School Business Manager and her team are responsible for handling all SARs, with the advice and guidance of the Data Protection Officer.

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests 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 School Business Manager.

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 carers 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.

A record of the Subjects Access Request and the subsequent disclosure will be retained for a period of 12 months and a record of each disclosure will be recorded on the SAR Register.

Children below the age of 13 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 our School 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.

Responding to subject access requests – Procedure
When responding to requests, we:

- Ensure the application is made using our '**Subject Access Request (Form)**'at **Appendix 1**
- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Request the Data Subjects permission to disclose the data to a parent or guardian
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

Collection will entail either:

- Collecting the data specified by the data subject, or
- Searching all databases and all relevant filing systems (manual files) of The Federation, including all back up and archived files, whether computerised or manual, and including all e-mail folders and archives. The ICT Lead maintains a data map that identifies where all data in the school is stored.

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
- Information covered by legal professional privilege
- Negotiations with the data subject in relation to the request
- Information for crime prevention or detection
- Management forecasts
- Information used for research, historical or statistical purposes

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee

which considers 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.

Supplying the data to the data subject
The information is provided to the data subject in electronic format unless otherwise requested and all the items provided are listed on the '**Responding to a Subject Access Request (Form)**' at **Appendix 2** that shows the data subject's name and the date on which the information is delivered.

The electronic formats used for responses to SARs are:
CSV files;
Excel files;
Word files;

All machine-readable transitions require a robust level of encryption to send the information to a data subject and or transmit that data to another controller, at the written request of the Data Subject.

Subject Access Request (Request Form)

[Insert date]

insert your school's name and address

Re: subject access request

Dear *School,*

Please provide me with the information about me that I am entitled to under the UK General Data Protection Regulation. This is so I can be aware of the information you are processing about me and verify the lawfulness of the processing.
Here is the necessary information:

Name	
Relationship with the School	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Correspondence address	
Contact number	
Email address	
Details of the information requested	Please provide me with: *Insert details of the information you want that will help us to locate the specific information. Please be as precise as possible, for example:* • *My personnel file* • *My child's medical records* • *My child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*

If you need any more information from me, please let me know as soon as possible.
Please bear in mind that, in most cases, you must supply me with the information within 1 month and is free of charge.

If you need any advice on dealing with this request, you can contact the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk

Yours sincerely,

[Insert Name]

Responding to a Subject Access Request (Form)

[Insert date]

Insert your school's name and address

Re: subject access request

Dear *insert the name of the individual who submitted the subject access request*

Please find enclosed the information that you requested under the UK General Data Protection Regulation (UK GDPR).

Your name	
Your relationship with the school	Please select: Pupil / parent / employee / governor / volunteer Other (please specify):
Details of the information you requested/enclosed	*Insert details of the specific information requested, such as:* • *Your personnel file* • *Your child's medical records* • *Your child's behaviour record, held by [insert class teacher]* • *Emails between 'A' and 'B' between [date]*
Date you requested the information	
Date we supplied the information	*This must be within one month of the above date*
Format we supplied the information	*For example, encrypted USB stick accompanying this letter*

[Ensure we send the data either manually or electronically and record a copy on the schools Server]

If you need any further advice relating to your subject access request, you can contact:

The School Business Manager on 01942 824 150 or Matthew Keeffe – Data Protection Officer – via matt@keeffeandassociates.co.uk .

Yours sincerely,

[Insert Name]

1. Scope

Where, in accordance with the UK GDPR, the consent of the data subject is required for the processing of his or her personal data, it will be within the scope of this procedure.
Consent of the data subject means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

2. Responsibilities

The data controller, The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) is responsible under the UK GDPR for obtaining consent from the data subject under advisement from the Data Protection Officer.

3. Consent procedure

3.1 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that the data subject has given explicit consent to the processing of his or her personal data (Consent Form – Pupil, Staff Member or Governor).

3.2 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that the data subject has consented to the processing of his or her personal data for one or more specific purposes (Consent Form – Pupil, Staff Member or Governor).

3.3 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that the data subjects' consent is easily distinguishable from any other matter relating to the data subject (if recorded in paper / electronic file format use the Consent Form – Pupil, Staff Member or Governor, or email then attach the email to the form).

3.4 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that the data subjects' consent is in an intelligible and easily accessible format using clear and plain language.

3.5 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that the data subject has been informed of their right to withdraw consent before giving consent.

3.6 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate that processing of data is limited to the contract bound by the explicit consent given by the data subject.

4. Withdrawal of consent procedure

4.1 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate the data subject has withdrawn consent to the processing of his or her personal data.

4.2 Where the processing had multiple purposes, The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) shall be able to demonstrate withdrawal of consent for all of them.

Annex D – Managing Subcontractors and 3rd Party's Process

1. Scope

All external suppliers that process personal data on behalf of The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) are within the scope of this procedure.

2. Responsibilities

2.1 The School Business Manager / Data Protection Officer in conjunction with the Finance team are responsible for approving the selection of all sub-contracted processors of personal data in line with the requirements of this procedure.

2.2 The owners of third-party relationships are responsible for ensuring that all data processing is conducted in line with this procedure.

2.3 The IT representative is responsible for ensuring that adequate technical and other resources that might be required are made available to support the relationship owner in the monitoring and management of the relationship.

2.4 The School Business Managers is responsible for conducting regular audits of contractor or third-party compliance.

3. Procedure

3.1 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) selects only suppliers that can provide technical, physical, and organisational security that meet The Federation's requirements in terms of all the personal information they will process on The Federation of Savile Town CE (C) and Thornhill Lees CE (VC)'s behalf.

3.2 Suppliers from outside the UK or EU will only be selected under the following conditions, in addition to the conditions noted elsewhere in this procedure.

3.2.1.1 If the supplier or the state in which it resides has been positively identified in an adequacy decision by the EU Commission or similar authority; or

3.2.1.2 Where there are legally binding corporate rules or Standard Contractual Clauses, and organizational and technical safeguards, established between The Federation and the supplier to secure the rights and freedoms of data subjects at least equal to those afforded within the EU; or

3.2.1.3 Where the arrangement has been approved by the Information Commissioner.

3.3 An information security risk assessment, is carried out before a supplier is engaged (See **Annex A**) and, if the School Business Manager considers it necessary because of the nature of the personal information to be processed or because of the particular circumstances of the processing, an audit of the supplier's security arrangements against the requirements of Cyber Essentials may be conducted before entering into the contract.

3.4 The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) requires a written agreement (See **Annex B**) to provide the service as specified and requires the supplier to provide appropriate security for the personal information it will process.

3.5 All data processing contracts allow The Federation to conduct regular audits of the supplier's security arrangements during the period in which the supplier has access to the personal information.

3.6 All data processing contracts forbid suppliers from using further subcontractors without The Federation's written authorization for the processing of personal information.

3.7 Contracts with second-level subcontractors will only be approved if they require the subcontractors to comply with at least the same security and other provisions as the primary subcontracting organisation (the supplier) if they specify that, when the contract is terminated, related personal information will either be destroyed or returned to The Federation of Savile Town CE (C) and Thornhill Lees CE (VC).

DRAFT LETTER AND INFORMATION SECURITY QUESTIONNAIRE FOR SUB CONTRACTORS AND 3RD PARTIES

Date:

[Insert Supplier Name and Address}

Dear Sir/Madam,

UK GDPR Compliance

As a School we are continually working towards ensuring compliance with the UK GDPR and the Data Protection Act 2018.

As a sub-contractor or 3rd party supplier you need to confirm that you have undertaken the necessary review of your processes and procedures to comply with the changes. To continue with our commercial relationship, we need confirmation of this and agreement that the current contract or arrangements will be agreed and amended to reflect this.

Please complete the series of questions below and explain how you will comply.

We require the form to be completed, signed, and returned to us. We reserve the right to request any additional information from you about your processes and procedures that will enable us secure compliance with the UK GDPR requirements.

As a public authority we have an obligation to be compliant with UK GDPR and to demonstrate compliance.

Thank you for your assistance.
Kind regards

[Insert Name and Job Title of person signing the letter]

School name:

To comply our arrangements with you under UK GDPR must ensure that you will:

Supplier Requirement	**Confirm consent and process**
Only use the data we provide or that you access from our organisation in accordance with our instructions,	
Ensure that anyone in your organisation understands that and data they have access to or use about our students or staff is confidential and must not be shared with anyone without our prior agreement	
Take all steps to keep the data secure, whether it is paper records, emails, digital or electronic. Please note we reserve the right to ask for evidence and details about how this is done.	
If you subcontract any part of the task, and personal information and data is required by that sub-contractor, you will seek and obtain our consent before proceeding.	
On occasion, we may receive a request to release information that we hold about an individual, whose data you have used or processed on our behalf. Please confirm that in those situations you will co-operate with us and provide all records about the person within a specified timeframe.	
Should there be a data breach, please confirm that you will notify us as soon as you are aware.	
In the event of a breach please confirm that you will co-operate with us to report, manage, and recover data that you have also had access to or use.	
In the event of a data breach, what is the process?	
You notify us if a breach occurs as soon as you become aware of it.	
That you will delete or return (at our choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);	
You will make available to the us all information necessary to demonstrate compliance; allow/contribute to audits (including inspections)	
Please provide answers to the following	
What processes do you have in place for testing the security of your system?	
When was this security system last tested and what was the outcome?	
What is your organisation's strategy for achieving compliance with the UK GDPR?	
Please provide details of your Data Protection/Information Security/Cyber Security Policy as appropriate	

I, ……. on behalf of …… confirm that the responses above are accurate and agree that this forms a written agreement and amendment to our current arrangement or contract with you.

Signed…….

Dated……...

Role within organisation……...

Dear [Insert Supplier Name],

DATA PROCESSOR AGREEMENT

We refer to the arrangement under which you (as the "**Supplier**") provide services to The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) ("**we**", "**us**", and "**our**"), including the terms and conditions applicable to that arrangement (as updated and amended from time to time) (the "**Terms**").

The UK General Data Protection Regulation (the "**UK GDPR"**) under the Data Protection Act 2018 (the "**DPA**") in regulating the processing of personal data.

As part of our arrangement, we will be forwarding data to you that must be processed in accordance with all applicable Data Protection Laws (including the DPA and UK GDPR). Article 28(3) of the UK GDPR specifies certain provisions which must be included in contracts between "controllers" and "processors" (such terms are defined in both the DPA and the UK GDPR). As such, this letter sets out the agreement between us to ensure the protection and security of data which we pass to you for processing.

Linked to this, you acknowledge that we are the data controller in respect of any personal data that you process while providing services for us.

AGREEMENT
In consideration for us forwarding to you such data, you agree to comply with all applicable Data Protection Laws and to use your best endeavours to ensure that by your actions you do nothing to compromise The Federation of Savile Town CE (C) and Thornhill Lees CE (VC) with the applicable Data Protection Laws.
With effect from the date of this letter, you confirm that:

1. The Data Protection Agreement and its Appendix at Annex 1 to this letter ("**Annex 1**") shall form a part of the Terms.

2. The provisions of Annex 1 shall replace any provisions in the Terms which expressly conflict, or are inconsistent, with any provisions of Annex 1. If there is any ambiguity between the provisions of the Terms (excluding this Data Processor Agreement) and this Data Processor Agreement, the provisions of this Data Processor Agreement shall prevail.

3. Except as set out in this letter, the Terms shall remain unchanged and shall continue in force.

NEXT STEPS
Please confirm the categories of personal data and data subjects in the Appendix to the Data Protection Agreement before signing and returning the enclosed copy of this letter (including a full copy of Annex 1) to acknowledge your agreement.

Yours faithfully

Signed ……
Name
For and on behalf of The Federation of Savile Town CE (C) and Thornhill Lees CE (VC)
Date ……

We agree to the provisions of the UK GDPR Addendum and the variation of the Agreement with effect from the Variation Date on the terms set out above.
Signed ……
Name ……

For and on behalf of ……
Date ……

Annex E – Data Protection Agreement

1. Definitions and interpretation

1.1 In this Agreement, unless the context otherwise requires, the following terms shall have the meanings set out below:

(a) "**School Personal Data"** means the Personal Data that you process on behalf of us under or in connection with the Terms;
(b) **"Data Protection Laws"** means all applicable data protection and privacy legislation, regulations and binding codes of practice issued by any DP Regulator, including the Data Protection Act 2018 (the "**DPA"**) and (the **"UK GDPR"**); the Privacy and Electronic Communications (EC Directive) Regulations 2003; and all legislation enacted in the UK in respect of the protection of Personal Data; in each case, to the extent in force, and as such are updated, amended, re-enacted or replaced from time to time;
(c) **"DP Regulator"** means any governmental or regulatory body or authority with responsibility for monitoring or enforcing compliance with the Data Protection Laws;
(d) **"Services"** means the products and/or services provided by you under the Terms and more particularly set out in the background to this Agreement;
(e) **"Standard Contractual Clauses"** shall mean the Standard Contractual Clauses annexed to the European Commission Decision (2010/87/EU) or any replacement thereof;
(f) **"Terms"** means all terms applicable to the legal relationship existing between the parties, including those individually negotiated and subject to written agreements, and under which you and your affiliates are hereafter identified as the "**Supplier**".

1.2 The terms **Data Subject**, **Personal Data**, **Personal Data Breach,** and **processing** shall have the meanings set out in the UK GDPR.

2. **Data protection**

2.1 The parties shall comply with the provisions and obligations imposed on them by the Data Protection Laws at all times when processing the School Personal Data in connection with the Terms.

2.2 The details of the processing of the School Personal Data carried out by the Supplier on our behalf are set out in the Appendix to this Agreement and form part of this Agreement (the "**Processing Instructions**").

2.3 Each party shall always maintain accurate, complete, and up-to-date written records of all processing operations under its responsibility that contain at least the minimum information required by the Data Protection Laws and shall make such information available to any DP Regulator on request.

2.4 The Supplier shall:

(a) process the School Personal Data only for the performance of the Services in accordance with the Terms and the Processing Instructions and/or our other written instructions from time to time;
(b) ensure that all its employees, officers, staff, agents, and sub-contractors who have access to the School Personal Data are informed of the confidential nature of the School Personal data and are subject to appropriate contractual obligations of confidentiality when processing such School Personal Data;
(c) implement and maintain technical and organisational measures and procedures to preserve the confidentiality and integrity of the School Personal Data and ensure an appropriate level of security for the School Personal Data, including protecting the School Personal Data against the risks of accidental, unlawful, or unauthorised processing, destruction, loss, alteration, disclosure, dissemination or access;
(d) only appoint a third party (including any subcontractors and affiliates) to process the School Personal Data with our prior written consent;

(e) where the Supplier sub-contracts any of its obligations to a sub-contractor who has been approved by us in accordance with clause 2.4(d), the Supplier shall enter into contractual data processing provisions with the sub-contractor, equivalent to those in place between the Supplier and us under this Agreement, for the duration of the sub-contractor's Processing of the School Personal Data.
(f) not transfer the School Personal Data outside the European Economic Area without our prior written consent and, where we provide such consent, the Supplier shall take such further actions as we direct (including entering into the Standard Contractual Clauses) to ensure that the transfer is subject to adequate safeguarding measures;
(g) inform us without undue delay if the School Personal Data is (while within the Supplier's or its subcontractors' or affiliates' possession or control) subject to a Personal Data Breach or is otherwise lost or destroyed or becomes damaged, corrupted or unusable;
(h) at our sole option, including on termination or expiry of the Terms or any part of them, return or irretrievably delete all the School Personal Data from all of the Supplier's software and/or hardware systems and, if applicable, procure that the School Personal Data is deleted from the software and/or hardware systems of the Supplier's employees, officers, staff, agents or subcontractors (as applicable) and not make any further use of the School Personal Data;
(i) at no additional cost, provide or make available to us and any DP Regulator such information and assistance as is reasonably required to verify, demonstrate, or ensure compliance with the Supplier's obligations (and each subcontractor's obligations, if applicable) in this Agreement and/or the Data Protection Laws;
(j) take such steps as are reasonably required to assist us in ensuring compliance with our obligations under Articles 30 to 36 (inclusive) of the UK GDPR;
(k) notify us within two (2) Business Days if it receives a request from a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data;
(l) provide us with such co-operation and assistance as may reasonably be required in relation to any request made by a Data Subject to exercise its rights under the Data Protection Laws in relation to that Data Subject's Personal Data; and
(m) not disclose any School Personal Data to any person or Data Subject other than at our written request or as expressly provided for in the Terms.

2.5 At our request and provided that we shall enter into appropriate confidentiality agreements (as reasonably required by the Supplier), the Supplier shall permit us or our representatives to access any relevant premises, personnel or records of the Supplier on reasonable notice to audit and otherwise verify the Supplier's compliance with its obligations under this this Schedule and the Data Protection Laws.

2.6 If either party receives any complaint, notice or communication which relates directly or indirectly to the processing of the School Personal Data by the other party or to either party's compliance with the Data Protection Laws, it shall as soon as reasonably practicable notify the other party and it shall provide the other party with reasonable co-operation and assistance in relation to any such complaint, notice or communication.

2.7 The Supplier shall indemnify us and keep us indemnified at its own expense against all claims, liabilities, damages, administrative fines, costs or expenses incurred by us or for which we may become liable due to any failure by the Supplier or its Sub-Processors, subcontractors, agents or personnel to comply with any of its obligations under this Schedule or under the Data Protection Laws.

3. **Law and jurisdiction**
3.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and interpreted in accordance with the laws of England and Wales.

3.2 The parties irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arise out of, or in connection with, this Agreement or its subject matter or formation.