

The Three Rivers Federation

Data Protection Policy

2025-2026

Version: 1.7

Policy Date: 3.12.2025

Approved by: The Three Rivers Full Governing Body

Next review date: 03.12.2025

Contents

1	Introduction and purpose	3
2	Scope.....	3
3	Definitions	4
4	Roles and responsibilities.....	4
4.1	Governing Body.....	4
4.3	Headteacher.....	4
4.5	Data Protection Officer	4
4.10	Employees, temporary staff, contractors, visitors.....	5
5	Data protection by design and by default	6
6	Data Protection Principles	6
7	Data subjects' rights.....	10
8	Personal data breaches.....	11
9	Sharing data	12
10	Data Protection Impact Assessments	13
11	Records management	14
	Policy history	15
	Data Protection Policy Definitions	24

1 Introduction and purpose

- 1.1 This policy sets out the Federation's commitment to handling personal data in line with the General Data Protection Regulation 2016 (UK GDPR) and the Data Protection Act 2018 (collectively referred to as the data protection legislation).
- 1.2 The Federation is the data controller for the personal data it processes and is registered with the Information Commissioner's Office (ICO) under registration number SC Z5916270 and CSM Z5361331. Details about this registration can be found at www.ico.org.uk
- 1.3 The purpose of this policy is to explain how the Federation handles personal data under the data protection legislation, and to inform employees and other individuals who process personal data on the Federation's behalf, of the Federation's expectations in this regard.

2 Scope

- 2.1 This policy applies to the processing of personal data held by the Federation. This includes personal data held about pupils, parents/carers, employees, temporary staff, governors, visitors and any other identifiable data subjects.

This policy should be read alongside the Federation's other policies, procedures and documentation, which refer to the handling of personal data:

[\[delete if not in place\]](#)

- Privacy Notice
- Appropriate Policy Document
- *Artificial Intelligence Acceptable Use Policy*
- IT Acceptable Use Policy
- Personal Data Breach Handling Procedure
- Data Protection Request Handling Procedure
- Education Record Request Handling Procedure
- Record Retention Schedule
- FOI Publication scheme

3 Definitions

3.1 There are several terms used in the data protection legislation and in this policy, which must be understood by those who process personal data held by the school. These are:

- Personal data
- Special categories of personal data
- Processing
- Data subject
- Data controller
- Data processor

3.2 These terms are explained in Appendix 1.

4 Roles and responsibilities

4.1 Governing Body

4.2 The Governing Body has overall responsibility for ensuring the Federation implements this policy and continues to demonstrate compliance with the data protection legislation. This policy shall be reviewed by the Governing Body on an annual basis.

4.3 Headteacher

4.4 The Headteacher has day-to-day responsibility for ensuring this policy is adopted and adhered to by employees and other individuals processing personal data on the Federation's behalf.

4.5 Data Protection Officer

4.6 The Data Protection Officer (DPO) is responsible for carrying out the following tasks:

- Informing and advising the Federation of their obligations under the data protection legislation
- Monitoring compliance with data protection policies
- Raising awareness and providing training
- Carrying out audits on the Federation's processing activities
- Providing advice regarding Data Protection Impact Assessments and monitoring performance
- Co-operating with the Information Commissioner's Office
- Acting as the contact point for data subjects exercising their rights

- 4.7 The Federation's DPO is Firebird Data Protection Consultancy Limited, an external company who performs the role under a service contract. The DPO can be contacted through the Federation at admin@stokecanon.devon.sch.uk or admin@csmmps.org.uk directly at DPO@firebirdltd.co.uk
- 4.8 The DPO is supported in their role by a Federation employee, this person is known as the Data Protection Link Officer. All enquiries, complaints, requests and suspected breaches of security, should be referred to the Data Protection Link Officer in the first instance, who will then notify the DPO. The Federation's Data Protection Link Officer email is admin@stokecanon.devon.sch.uk or admin@csmmps.org.uk
- 4.9 The DPO reports directly to the governing body and Senior Leadership Team and shall provide regular updates on the Federation's progress and compliance with the data protection legislation.
- 4.10 **Employees, temporary staff, contractors, visitors**
- 4.11 All employees, temporary staff, contractors, visitors and others processing personal data on behalf of the Federation, are responsible for complying with the contents of this policy. Failure to comply with this policy may result in disciplinary action or termination of employment or service contract.
- 4.12 All employees, temporary staff, contractors, visitors shall remain subject to the common law duty of confidentiality when their employment or relationship with the Federation ends. This does not affect an individual's rights in relation to whistleblowing. On termination of employment, employees shall return all information and equipment to the Federation, including personal identification passes/smart cards and keys.
- 4.13 Unauthorised access, use, sharing or procuring of the Federation's data may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.
- 4.14 Employees shall have no expectation of privacy in their use of the Federation's systems. Any correspondence, documents, records or handwritten notes created for work related purposes, may be disclosable to data subjects or the public under the UK General Data Protection Regulation, the Freedom of Information Act 2000 or Environmental Information Regulations 2004.
- 4.15 The Federation reserves the right to monitor employees' use of the Federation's systems and where necessary access work related emails and messages sent from work accounts, This may be done without notice. Employee monitoring and access to data will only be carried out where this is considered necessary and proportionate, for example to discharge the Federation's statutory duties in relation to safeguarding, health and safety, statutory reporting and responding to information requests. It may also be carried out for security purposes, to identify suspicious activity, compliance with Federation policies, quality checking and training purposes.

5 Data protection by design and by default

- 5.1 The Federation is committed to ensuring that data protection considerations are at the heart of everything it does involving personal data, and shall ensure that it has appropriate technical and organisational measures in place which are designed to implement the Data Protection Principles in an effective manner.
- 5.2 The Federation shall ensure that by default, it will only process personal data where it is necessary to do so, and appropriate safeguards are in place to protect it. This Data Protection Policy and supplementary policies, procedures and guides demonstrate how the Federation achieves their 'data protection by design and default' obligations.

6 Data Protection Principles

- 6.1 The UK GDPR provides a set of 6 principles which govern how the Federation handles personal data. These are set out in Article 5 of the UK GDPR. All employees, temporary staff, contractors, and other individuals processing personal data on behalf of the Federation are responsible for complying with the data protection principles:
- 6.2 **1) Personal data shall be processed lawfully, fairly and in a transparent manner** (*'lawfulness, fairness and transparency'*).
- 6.3 This means personal data shall only be processed where there is a lawful basis which allows this; we are fair to data subjects when we use or share their personal data (ie we must act in a way they would reasonably expect); and are transparent in how we handle personal data by describing this in our privacy notices. The Federation's privacy notices are available at SC website click [here](#) or CSM click [here](#)
- 6.3 The data protection legislation lists the different lawful bases which permit the collection, use and sharing etc of personal data. These are contained in Article 6 of the UK GDPR. At least one of these legal bases must apply when processing personal data. In summary:
- The data subject has given consent.
 - It is necessary for contractual purposes.
 - It is necessary to comply with a legal obligation.
 - It is necessary to protect someone's life.
 - It is necessary to carry out a task in the public interest or exercise our official duties.
 - It is necessary to pursue the Federation's legitimate interests or a third party's legitimate interests, except where such interests are overridden by the data subject, in particular, where the data subject is a child.
- 6.4 When 'special categories' of personal data are processed (ie data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data; health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list:
- The data subject has given explicit consent.

- The processing is necessary for employment, social security or social protection purposes (e.g. safeguarding individuals at risk; protection against unlawful acts; prevention against fraud).
- It is necessary to protect the data subject's life and they are physically or legally incapable of giving consent.
- The data subject has made the information public.
- The processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- The processing is necessary for reasons of substantial public interest and are proportionate to the aim pursued.
- The processing is necessary for health or social care purposes.
- The processing is necessary for reasons of public interest in public health.
- The processing is necessary for archiving purposes in the public interest, scientific or historical research or statistical purposes.

6.5 Although consent is one of the lawful bases that can be relied upon when processing personal data or special category data, it is not appropriate to rely on this for most of the processing the Federation does. This is because there is a high standard for achieving 'valid' consent and there are potential difficulties for the Federation should the data subject later withdraw their consent to the processing. The Federation shall therefore look for alternative lawful bases to legitimise its processing where they are more appropriate, such as *'processing is necessary to carry out a task in the public interest or exercise official duties'* and *'processing is necessary for the purposes of employment, social security or social protection'*.

6.6 There are however circumstances when the Federation is required to obtain consent to process personal data, for example:

- To collect and use biometric information (eg fingerprints and facial images) to be used for identification purposes.
- To send direct marketing or fundraising information by email or text, where the data subject would not have a reasonable expectation that their data would be used in this way or has previously objected to this.
- To take and use photographs, digital or video images and displaying, publishing or sharing these in a public arena (such as on social media, on the Federation website; in the Press; in the prospectus; newsletter etc), where the data subject would not have a reasonable expectation that their images would be used in this way, or the rights of the data subject override the legitimate interests of the Federation.
- To share personal data with third parties (e.g. professionals, agencies or organisations) where the data subject has a genuine choice as to whether their data will be shared, for example when offering services which the data subject does not have to accept or agree to receive.

- 6.7 Where it is appropriate for the Federation to use consent as its lawful basis, it shall ensure the person providing it has positively opted-in to the proposed activity and is fully informed as to what they are consenting to and any non-obvious consequences of giving or refusing that consent.
- 6.8 Consent shall not be assumed as being given if no response has been received e.g. a consent form has not been returned. Where consent is being obtained for the collection or use of children's information, consent shall be obtained from a parent or guardian until the child reaches their 13th birthday. Consent shall be obtained directly from children aged 13 years and over where those children are deemed by the Federation to have sufficient maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).
- 6.9 The Federation shall ensure that where consent is obtained, there is a record of this. Where possible, consent shall be obtained in writing. All forms requesting consent shall include a statement informing the person of their right to withdraw or amend their consent, and instructions on how to do this easily.
- 6.10 **2) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').**
- 6.11 This means the Federation shall only collect and use personal data for the reasons specified or described in its privacy notices and shall not process this data in any way which could be considered incompatible with those purposes, in other words, using the data for a different or unexpected purpose.
- 6.12 **3) Personal data shall be adequate, relevant and limited to what is necessary for the purpose it was processed ('data minimisation').**
- 6.13 This means the Federation shall ensure that any personal data collected, used or shared etc. is fit for purpose, relevant and not excessive or disproportionate for the purpose it was intended.
- 6.14 **4) Personal data shall be accurate and where necessary kept up to date; every reasonable step must be taken to ensure that inaccurate personal data are erased or rectified without delay ('accuracy').**
- 6.15 This means the Federation shall take all reasonable efforts to ensure the personal data it holds is accurate and where necessary kept up to date, and where personal data is found to be inaccurate, this information shall be corrected or erased without delay.
- 6.16 The Federation shall send reminders, on at least an annual basis, to parents/carers, pupils and employees, asking them to notify the Federation of any changes to their contact details or other information. The Federation shall also carry out periodic sample checks of pupil and employee files to ensure the data is accurate and up to date.
- 6.17 **5) Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed ('storage limitation').**

- 6.18 This means the Federation shall not keep personal data for any longer than it needs to. Personal data may be stored for longer periods where it is solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, provided that appropriate technical and organisational measures are in place to safeguard the rights and freedoms of the data subject.
- 6.19 The Federation shall maintain and follow a Record Retention Schedule which sets out the timeframes for retaining and disposing of personal data. This schedule shall be published alongside the Federation's privacy notices on the website [SC click here](#) and [CSM click here](#)
- 6.20 The Federation shall designate responsibility for record retention and disposal to data leads, who shall adhere to the Federation's Record Retention Schedule [click here](#) and ensure the timely and secure disposal of the data.
- 6.21 **6) Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. ('integrity and confidentiality)**
- 6.22 This means the Federation shall have appropriate security in place to protect personal data. The following are examples of the minimum technical and organisational measures that shall be in place to protect personal data:
- 6.23 **Technical security measures:**
- Security patches shall be applied promptly.
 - Access to systems shall be restricted according to role-based requirements.
 - Strong password policies shall be enforced; passwords shall be a minimum of 8 characters in length; changed at appropriate intervals and not shared or used by others. Password managers shall be utilised where possible.
 - Portable devices (such as laptops) and removable media (such as USBs) storing personal data shall be encrypted.
 - Data shall be backed up regularly.
 - The Federation's disaster recovery and business continuity plans shall be regularly tested to ensure data can be restored in a timely manner in the event of an incident.
 - Two factor authentication (2FA) shall be enabled on systems containing sensitive data.
- 6.24 **Organisational security measures:**
- Employees shall sign confidentiality clauses as part of their employment contract.
 - Mandatory data protection awareness training shall be provided to employees and governors during on-boarding and annually thereafter.
 - Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.

- Policies and guidance shall be communicated to employees and governors on the secure handling of personal data in Federation and when working remotely.
- Data protection compliance shall be a regular agenda item in governing body and Senior Leadership Team meetings. All employees shall be given the opportunity to raise compliance queries or concerns at any meeting.
- Cross cutting shredders and/or confidential waste containers will be available on the Federation's premises and used to dispose of paperwork containing personal data.
- Appropriate equipment and guidance will be available for employees to use and follow when carrying confidential paperwork off Federation premises.
- The Federation's buildings, offices and where appropriate classrooms, shall be locked when not in use.
- Paper documents and files containing personal data shall be locked in cabinets/cupboards when not in use, and access restricted on a need to know basis.
- Procedures shall be in place for visitors coming onto the Federation's premises. These will include signing in and out at reception, wearing a visitor's badge and being escorted where appropriate.
- The Federation shall have procedures in place to identify, report, record, investigate and manage personal data breaches in the event of a security incident.
- The Federation shall have procedures in place to effectively wipe all data from redundant computer equipment (to include smartphones, tablets, cameras, memory cards, photocopiers, multi-function devices, CDs, USBs etc) prior to their decommissioning, re-use or disposal. The equipment shall be stored in a secure area pending their collection by disposal companies.

6.25 The Federation shall have appropriate records in place to demonstrate compliance with each of these data protection principles ('accountability').

7 Data subjects' rights

7.1 Data subjects have several rights under the data protection legislation. The right to:

- be told how their personal data is being processed;
- request access to their personal data;
- request that inaccurate or incomplete personal data is rectified;
- request the erasure of personal data in certain circumstances;
- request the processing of their personal data is restricted in some circumstances;
- request that their personal data is transferred from one organisation to another or given to them, in certain circumstances;
- object to their personal data being used for public interest or direct marketing purposes;

- prevent important decisions being made about them by solely automated means (including profiling);
 - complain to the Federation about the handling of their personal data. If they remain dissatisfied with Federation's response, they have the right to escalate this to the Information Commissioner's Office.
- 7.2 Data subjects may exercise their data protection rights by contacting the Federation in writing or verbally. Data subjects are recommended to submit their request in writing and send this to admin@stokecanon.devon.sch.uk or admin@csmmps.org.uk or telephone SC 01392 841279 or CSM 01392 874583. The Federation shall handle all Data Protection Requests in line with the Data Protection Request Handling Procedure.
- 7.3 Requests from parents seeking access to their child's education record, shall be handled under The Education (Pupil Information) (England) Regulations 2005 and the Federation's Education Record Request Handling Procedure.

8 Personal data breaches

- 8.1 The Federation shall follow the Personal Data Breach Handling Procedure in the event of a personal data breach. A personal data breach is a:

'breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed'.

- 8.2 Examples of personal data breaches include, but are not limited to:
- Entering or uploading personal data about identifiable individuals into artificial intelligence (AI) tools which have not been assessed and approved by the Federation.
 - Emailing a group of parents and failing to insert their private email addresses into the 'Bcc' field, thus revealing those email addresses to all recipients.
 - Emailing or posting confidential information to the wrong person.
 - Not storing or disposing of confidential paperwork securely.
 - Loss or theft of IT equipment which has personal data stored on it eg a laptop, iPad, mobile phone or a USB.
 - Altering, sharing or destroying personal data records without permission from the Federation.
 - Using another person's login credentials to gain higher level access to records.
 - Sharing login details or having insufficient access controls to systems, which result in unauthorised viewing, use, modification or sharing of personal data.
 - Hacking into a system containing personal data.
 - A social engineering incident whereby a person uses deception to manipulate individuals into divulging confidential or personal information eg a phishing email.
 - A cyber-attack resulting in loss of access to personal data (eg a ransomware attack).
 - Environmental incidents such as a fire or flood which damage or destroy important personal data records, prior to their scheduled disposal.
 - An employee abusing their access privileges to look at someone else's records out of personal curiosity or gain.

- 8.3 All personal data breaches and suspected breaches (including cyber incidents) shall be reported to the Data Protection Officer immediately, via the Federation's Data Protection Link Officer, by emailing admin@stokecanon.devon.sch.uk or admin@csmps.org.uk or telephone SC 01392 841279 or CSM 01392 874583 or directly to dpo@firebirdltd.co.uk
- 8.4 All incidents shall be recorded on the Federation's personal data breach log and investigated by a member of the Senior Leadership Team (or other person as appropriate), under the support and direction of the Data Protection Officer. Cyber incidents shall be reported to and investigated by the Federation's IT Manager or Security Manager who shall keep the Data Protection Officer informed of their findings where personal data has been compromised.
- 8.5 **Notification to the ICO and Data Subjects**
- 8.6 The Data Protection Officer shall determine whether the Federation must notify the Information Commissioner's Office and data subjects following a personal data breach.
- 8.7 A personal data breach is required to be reported to the ICO within 72hrs of the Federation becoming aware of the breach, where the breach is likely to result in a risk to the data subject or someone else, for example if they are likely to suffer damage, discrimination, disadvantage or distress.
- 8.8 Data subjects are required to be informed without undue delay, where the breach is likely to result in 'high risks', for example if the breach could lead to identity theft, psychological distress, humiliation, reputational damage or physical harm.
- 8.9 The Data Protection Officer shall notify the ICO (following consultation with the Federation) where a personal data breach meets the 'risk' threshold. The Headteacher or other delegated employee shall notify data subjects (or their parents) following a 'high risk' breach.

9 Sharing data

- 9.1 The Federation regularly shares personal data internally and externally with partner agencies and third parties for legitimate purposes. Employees shall follow to the Federation's policies and procedures when sharing personal data and adhere to the statutory and non-statutory guidance as set out in the:
- HM Government: Information Sharing Advice for Safeguarding Practitioners (2024)
 - Department for Education: Keeping Children Safe in Education (2025)
 - Information Commissioner Office: Data Sharing Code of Practice (2021)
- 9.2 When sharing personal data with third parties the Federation shall adhere to the following principles:
- Data subject(s) shall be made aware of the sharing through privacy notices or specific communications regarding the sharing.
 - An appropriate lawful basis shall be identified prior to the sharing.
 - Data shared shall be adequate, relevant and limited to what is necessary.

- Accuracy of the data shall be checked prior to the sharing (where possible).
- Expectations regarding data retention shall be communicated.
- Data shall be shared by secure means and measures in place to protect the data when received by the third party.
- A record shall be kept of the data sharing, including decisions not to share.
- Information sharing agreements shall be in place where required.

9.3 The Federation understands the data protection laws expressly allow organisations to share necessary and proportionate personal data with third parties to protect the safety or well-being of a child and in urgent or emergency situations to prevent loss of life or serious physical, emotional or mental harm, and is not a barrier to sensible and necessary sharing.

9.4 **Sharing data with suppliers (data processors)**

9.5 The Federation uses a variety of service providers to help it run effectively. These are sometimes referred to as 'data processors'. This often includes companies providing services such as IT support, professional advice, learning or teaching resources, management information systems, parent communication platforms, document storage solutions, Artificial Intelligence platforms, visitor entry systems, facial recognition and biometric data storage systems, HR and payroll platforms.

9.6 Using these service providers usually requires disclosing personal data to them so they can deliver the service or product the Federation has purchased or subscribed to. The data protection legislation requires that before sharing personal data with a service provider, the Federation must carry out due diligence checks on the company or product, to assess they have appropriate measures in place that ensures compliance with the data protection legislation and protects the rights of data subjects.

9.7 Due diligence checks shall be carried out on prospective service suppliers by the Federation, alongside the Data Protection Officer prior to using the service or product provided by the supplier. The outcome shall be recorded on the Federation's Data Processor Due Diligence Report template.

9.8 Employees shall not purchase a product or service which involves the disclosure of personal data, unless the appropriate due diligence checks have been carried out in consultation with the Data Protection Officer, a data processing agreement (or equivalent) is in place, and the product has been approved by a member of SLT (or other delegated person).

10 **Data Protection Impact Assessments**

10.1 The Federation is required to carry out Data Protection Impact Assessment (DPIAs) on the processing of personal data, where this is likely to result in 'high risks' to the rights and freedoms of data subjects. High risk means the potential for any significant physical, material or non-material harm (eg distress) to individuals.

- 10.2 A DPIA is a process which helps the Federation identify, minimise and document the data protection risks of a project or plan involving personal data. It demonstrates the Federation's compliance with the data protection principles and fulfils its 'accountability' and 'data protection by design' obligations. A DPIA does not have to eradicate all risk, but should minimise risks and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what the Federation wants to achieve.
- 10.3 The UK GDPR sets out three types of processing which will always require a DPIA:
- Systematic and extensive evaluation or profiling of individuals with significant effects
 - Large scale use of sensitive data (special category or criminal conviction or offence data)
 - Systematic monitoring of a publicly accessible area on a large scale
- 10.4 The Federation shall follow the Information Commissioner's Office supplementary list of processing, which also requires a DPIA:
- Use of innovative technology (including the use of Artificial Intelligence (AI) tools)
 - Denial of a service, opportunity or benefit
 - Large scale profiling
 - Processing of biometric or genetic data
 - Data matching
 - Invisible processing
 - Tracking
 - Targeting children or other vulnerable individuals
 - Risk of physical harm
- 10.5 The Federation shall also consider the European guidelines (Guidelines on Data Protection Impact Assessment), to help identify other likely high risk processing, which includes:
- Use of sensitive data or data of a highly personal nature.
 - Data concerning vulnerable data subjects.
 - Innovative use or applying new technological or organisational solutions.
- 10.6 The Federation shall use their DPIA pre-screening checklist to help identify whether a DPIA should be carried out. The results from DPIAs shall be recorded and shared with the Data Protection Officer, who will advise on any privacy risks and mitigations that can be made to reduce the likelihood of these risks materialising. The Data Protection Officer will monitor the outcome of the DPIA to ensure the mitigations are put in place. DPIAs shall be reviewed on an annual basis.

11 Records management

- 11.1 Records management is a system for managing records throughout their life cycle, from the time of creation or receipt to their destruction. The Federation recognises that good records management plays a crucial role in the smooth running of the Federation and is also necessary to comply with its obligations under the data protection legislation and the Freedom of Information Act 2000, particularly when responding to information access requests and protecting personal data from security threats.
- 11.2 The Federation shall manage its electronic and paper-based records in line with the statutory Code of Practice on the Management of Records, issued under section 46 of the Freedom of Information Act 2000.
- 11.3 Employees and governors shall be provided with advice, guidance and training on how to manage the Federation's records effectively throughout their lifecycle. This should include naming, storing, accessing, security classification, and disposal of records.
- 11.4 The Federation shall maintain a record retention schedule and regularly review its records to ensure they are disposed of in line with the schedule. The schedule shall be communicated to data leads responsible for managing the Federation's records.
- 11.5 **Record of processing activities**
- 11.6 The Federation shall, amongst other things, know what personal data records it holds, who it shares these records with; the security in place to protect them and how long they are to be kept for. This information shall be recorded in a Record of Processing Activities Inventory (ROPA), in line with Article 30 of the UK GDPR. The ROPA shall be reviewed annually and made available to the Information Commissioner upon request.

Policy history

Policy Version and Date	Summary of Change	Amended by	Implementation Date
Version 1.7	- Throughout document – simplified and amended paragraph numbering - Page 1 – date changes - Para 2.2 - insertion of: bullet points '<i>privacy notice</i>'; '<i>Artificial Intelligence Acceptable Use Policy [delete if not in place]</i>' - Para 4.15 – insertion of: '<i>and CCTV footage following incidents or complaints</i>'; '<i>and images</i>' - Para 8.2 – insertion of: '<i>Entering or uploading personal data about identifiable individuals into artificial intelligence (AI) tools which</i>	Firebird Data Protection Consultancy (Data Protection Officer)	Xx/xx/2025

	<i>have not been assessed and approved by the Federation’.</i> • Para 9.1 – date changes • Para 9.2 – insertion of: <i>‘including decisions not to share.’</i> • Para 9.8 – insertion of: <i>‘(or equivalent)’</i> • Para 10.4 – insertion of: <i>‘tools’</i>		
Version 1.6	• 2.2 Insertion of an additional bullet point: <i>‘Appropriate Policy Document’</i> • 4.5.5 Insertion of new paragraph: <i>‘The Federation reserves the right to monitor employees’ use of the Federation’s systems and where necessary access work related emails and messages sent from work accounts. This may be done without notice. Employee monitoring and access to data will only be carried out where this is considered necessary and proportionate, for example to discharge the Federation’s statutory duties in relation to safeguarding, health and safety, statutory reporting and responding to information requests. It may also be carried out for security purposes, to identify suspicious activity, compliance with Federation policies, quality checking and training purposes.’</i> • 6.25 Insertion of new bullet point: <i>‘The Federation shall have procedures in place to effectively wipe all data from redundant computer equipment (to include smartphones, tablets, cameras, memory cards, photocopiers, multi-function devices, CDs, USBs etc) prior to their decommissioning, re-use or disposal. The equipment shall be stored in a secure area pending their collection by disposal companies.’.</i> • 8.3 Insertion of addition wording: <i>‘or directly to dpo@firebirdltd.co.uk’</i> • 9.1 DfE and ICO guidance dates updated • 9.4.1 Paragraph amended:	Data Protection Officer	Xx xx 2024

	<i>The Federation uses a variety of service providers to help it run effectively. These are sometimes referred to as 'data processors'. This often includes companies providing services such as IT support, professional advice, learning or teaching resources, management information systems, parent communication platforms, document storage solutions, Artificial Intelligence platforms, visitor entry systems, facial recognition and biometric data storage systems, HR and payroll platforms.</i> • 9.4.2 Insertion of '<i>or subscribed to.</i>' • 9.4.3 Insertion of '<i>prior to using the service or product provided by the supplier</i>' • 9.4.4 Insertion of '<i>a data processing agreement is in place</i>' • 10.4 Insertion of '<i>including the use of</i>'		
Version 1.5	This policy has been re-written to simplify and re-order the existing content and includes new content (Records Management). This policy replaces the Federation's existing Data Protection Policy in its entirety.	Data Protection Officer	Xx xx 2023
Version 1.4	• 5.2.2 all bullet points re-worded and simplified • 5.2.3 all bullet points re-worded and simplified • 5.2.6 all bullet points re-worded • 5.8.1 insertion of new bullet point - <i>use of two factor authentication (2FA) on accounts containing sensitive data</i> • 5.9.1 following bullets point re-worded- <i>Data protection awareness training shall be provided to employees during on-boarding and annually thereafter.</i> <i>Policies and guidance shall be in place relating to the secure handling of personal data whilst in Federation and when working remotely outside of Federation.</i>	Data Protection Officer	Xx xx 2022

	• 5.9.1 new bullet point- <i>Cyber security training, guidance or advice shall be cascaded to employees on a regular basis.</i> • 5.10.2 following bullet point re-worded- <i>Have inaccurate or incomplete data corrected</i> • 5.14.2 sentence re-worded – <i>Due diligence checks on prospective data processors shall be carried out alongside the Data Protection Officer. A record shall be kept of the Federation’s findings.</i> • 5.15.1 following bullet point re-worded- <i>Purposes of the processing and any recipients of the data (including data processors)</i> • 5.17 entire section re-worded • 5.18 insertion of a new section		
Version 1.3	• 1.1 – removal of the reference ‘EU GDPR’ changing this to ‘UK GDPR’ • 2.2 – amended to read: <i>This policy should be read alongside the Personal Data Breach Handling Procedure, Data Protection Request Handling Procedure and [insert other relevant policies and procedures such as the E-Safety Policy; ICT Policy, CCTV Policy, Acceptable Use Policy etc].</i> • 4.4.4 – insertion of new sentence to read - <i>All individuals who handle the Federation’s data shall be made aware that unauthorised access, use, sharing or procuring of data, may constitute a criminal offence under the Data Protection Act 2018 and/or the Computer Misuse Act 1990.</i> • 5.1.2 – insertion of new sentence to read: <i>The Federation shall have appropriate measures and records in place to demonstrate compliance with the data protection principles.</i> • 5.1.3 – renumbering of existing paragraph	Data Protection Officer	xxxxx

	• 5.2.2 – insertion of new bullet point to read: <i>It is necessary for the legitimate interests of the Federation (where applicable) or third party, except where such interests are overridden by the data subject</i> • 5.14.2 – re-wording of paragraph to read: <i>Due diligence checks on prospective data processors shall be carried out as part of the Federation’s Data Protection Impact Assessment (DPIA) process. A record shall be kept of the Federation and Data Protection Officer’s findings on a DPIA report.</i> • 5.14.3 – insertion of the phrase ‘UK GDPR’ • 5.15.1 insertion of the phrase ‘UK GDPR’ • 5.15.2 re-wording of paragraph to read: <i>This inventory shall be reviewed annually and made available to the Information Commissioner upon request.</i> • 5.16.1 re-wording of paragraph to read: <i>The Federation shall follow the Personal Data Breach Handling Procedure in the event of a personal data security breach. These include incidents resulting in the:</i> • <i>unauthorised or accidental disclosure or access to personal data</i> • <i>unauthorised or accidental alteration of personal data</i> • <i>accidental or unauthorised loss of access or destruction of personal data</i> • 5.16.2 re-wording of paragraph to read: <i>All personal data security breaches and suspected breaches must be reported to the Data Protection Officer immediately, via the Federation’s Data Protection Link Officer, by emailing [insert Federation email address] or telephone [insert Federation number].</i>		
--	---	--	--

	• 5.16.6 re-wording of paragraph to read: <i>Where a breach is likely to result in a risk to the data subject, for example if they could suffer damage, discrimination, disadvantage or distress as a result of the breach, the Data Protection Officer shall notify the Information Commissioner's Office (ICO), within 72hrs of the Federation becoming aware of the breach.</i> • 5.18.1 insertion of the phrase 'UK GDPR' • Removal of employee declaration form at the end of the policy		
Version 1.2 July 2020	• 5.2.3 – amended to read: <i>When special categories of personal data are processed (ie data which reveals a person's racial or ethnic data; political opinions; religious or philosophical beliefs; trade union membership; genetic or biometric data (eg fingerprints); health data; sex life or sexual orientation), this shall only be done where a lawful basis has been identified from the list above, and one from the following list...</i> • 5.2.11 – amended to read: <i>The Federation's privacy notices shall be clear, concise, easily accessible and published on the Federation's website. All forms collecting personal data shall include reference to the Federation's privacy notices and a link provided to their location.</i> • The following paragraphs have been removed: 5.2.12; 5.2.13; 5.2.14 • 5.5.3 – amended to read: <i>The Federation shall carry out periodic sample checks of pupil and employee files containing personal data, to ensure the data is accurate and up to date.</i> • 5.10.1 – amended to read: <i>Data subjects have several rights under the data protection legislation. The Federation shall comply with all valid requests (written or verbal) from data subjects exercising their rights without delay, and within one month at the latest.</i> • 5.10.2 – bullet points have been re-worded in full	Data Protection Officer	xxxxx

	• 5.11.1 – amended to read: <i>Data subjects exercising their rights are recommended to put their request in writing and send it to the Federation at [insert Federation postal address and email address]. Data subjects can also exercise their rights verbally. Requests shall be handled in line with the Federation’s Data Protection Request Handling Procedure.</i> • The following paragraphs have been removed: 5.11.2; 5.11.3; 5.11.4; 5.11.5; 5.11.6; 5.11.7; 5.11.8 • 5.14.2 has been amended to read: <i>The Federation’s Data Protection Officer, IT Manager and Data Protection Link Officer shall assess the appropriateness of data processors before the Federation purchases their services. A record will be kept of their findings on a Data Processor Due Diligence Report.</i>		
Version 1.1 1 July 2019	• Version number and policy date (page 1) • 2.2 amended to read <i>[insert relevant policies and procedures such as the E-Safety Policy; ICT Policy etc].</i> • 4.2 amended to read: <i>Headteacher [or Principal]</i> • 4.2.1 amended to read: <i>The Headteacher [or principal]</i> • 4.3.3 amended to read: <i>The DPO is Amber Badley, who can be contacted through the Federation at [insert Federation email address] or directly via DPO@firebirdltd.co.uk</i> • 5.2.7 amended to include: <i>Where consent is being obtained for the collection or use of children’s information, consent shall be obtained from a parent or guardian until the child reaches the age of 12. Consent shall be obtained directly from children aged 13 years and over, where those children are deemed by the Federation to have sufficient</i>	Data Protection Officer	xxxxx

	<i>maturity to make the decision themselves (except where this is not in the best interests of the child. In such cases, consent will be obtained from an adult with parental responsibility for that child).</i> • 5.2.12 amended to read: <i>This notice will be published on the Federation's website; parents will be directed to this on an annual basis.</i> • 5.2.13 amended to read: <i>Employees will be given a privacy notice explaining how the Federation handles employee information when they join the Federation and directed to this annually thereafter.</i> • 5.11.1 amended to read: <i>Data subjects exercising their rights are recommended to put their request in writing and send it to the Federation at [insert Federation postal address and email address]. Data subjects can also exercise their rights verbally. In such cases, the Federation will promptly write to the data subject outlining the verbal discussion/request and will ask the data subject to confirm this is accurate.</i> • Renumbering of paragraphs in section 5.11-5.12 • 5.11.4 amended to read: <i>Pupils can request access to their own personal data when they have sufficient maturity to understand their rights; know what it means to make such a request and can interpret the information they receive. The Information Commissioner's Office and the Department for Education guidance, suggests that children aged 13 years and above, may have sufficient maturity in these situations, however it is for the Federation to decide this on a case by case basis.</i>		
Version 1.0 25 May 2018	This policy replaces the Federation's existing Data Protection Policy	Data Protection Officer	25 May 2018

Data Protection Policy Definitions

Term Used	Summary Definition
Personal data	Personal data means any information relating to an identified or identifiable living individual. This includes a name, identification number, location data, an online identifier, information relating to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
Special categories of personal data	Special categories of personal data mean personal data which reveal the racial or ethnic origin, political opinions, religious or philosophical beliefs and the trade union membership of the data subject. It also includes the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, and data relating to an individual's sex life or sexual orientation.
Processing	Processing means any operation or set of operations which is performed on personal data, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Data subject	An identifiable, living individual who is the subject of personal data.
Data controller	A data controller is an organisation who determines the purposes and means of the processing of personal data.
Data processor	A data processor is an individual or organisation who processes personal data on behalf of a data controller, upon their instructions.