The Winterton Federation
Data Protection Policy

Name and title of Author/s:	Tim Pinto and Cheryl Baxter
Name of responsible Committee/individual:	Keeping Safe and Well Committee
Updated:	Spring 2026
Review date:	Spring 2028
Targeted audience:	Staff/parents/governors
Related documents: All federation policies referred to are available on the federation website: https://thewintertonfederation.co.uk If English is not your first language, and you require assistance/translation, please contact the Junior school office.	UK-GDPR Data Protection Act (2018) School Standards and Framework Act 1998 Freedom of Information Act 2000 Electronic Commerce (EC Directive) Regulations 2002 The Privacy and Electronic Communications (EC Directive) Regulations 2003 The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018) Protection of Freedoms Act 2012 Data Access & Use Act 2025 (DUAA) Employment Rights Act (1996) 'Guide to the UK General Data Protection Regulation (UK-GDPR)' 'IT asset disposal for organisations' 'Data protection: a toolkit for schools' DfE (2015) 'Keeping Children Safe in Education' Freedom of information publication scheme Safeguarding Policy Information Security Policy Data Breach Policy E-Safety Policy Bring Your Own Device Agreement CCTV Policy Artificial Intelligence Policy Acceptable Use Agreement Cyber Response Plan
Strategic alignment:	1.4 Objective: Continue to maintain a safe working and learning environment

Contents

Aims 3
Legislation and Guidance 3
Definitions 4
The Data Controller 5
Roles and Responsibilities 5
- Governing board 5
- Data Protection Officer 5
- Executive Headteacher 5
- All staff 5

Data Protection Principles 6
Collecting Personal Data 6

- Lawfulness, fairness and transparency 6
- Limitations, minimisation and accuracy 7

Sharing Personal Data 8
Subject access requests and other rights of individuals 8
- Subject access requests 8
- Children and subject access requests 9
- Responding to subject access requests 9
- Other data protection rights of the individual 10
- Parental requests to see the educational record 10
- Photographs and Videos 11
- Data protection by design and default 11

Data Security 12
Artificial Intelligence 12
Personal Data Breaches 12
Safeguarding 13
DBS Data 13
Training 13
Monitoring arrangements 13

“TO BE THE BEACON FOR LEARNING”
“Let your light shine so others may see your good deeds|” Matthew 5:16.

Aims

Our federation aims to ensure that all personal data collated about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with relevant legislation.

With recent changes to the UK's relationship with the European Union, the policy reflects the UK-GDPR (General Data Protection Regulation) and the Data Protection Act (2018).

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

Legislation and guidance

This policy meets the requirements of the UK-GDPR and DPA 2018. The policy reflects guidance issued by the Information Commissioner and Information and Records Management Society.

In addition, the policy sets out good practice issued by the National Cyber Security Centre on the security of electronic data.

It also reflects the Information Commissioner's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with our funding agreement and articles of association.

The policy covers the following legislation:

- The UK General Data Protection Regulation (UK-GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- Data Access & Use Act 2025 (DUAA)
- Employment Rights Act (1996)

This policy also has regard to the following guidance:

- ICO (2021) 'Guide to the UK General Data Protection Regulation (UK-GDPR)'
- ICO (2012) 'IT asset disposal for organisations'
- DfE (2018) 'Data protection: a toolkit for schools'
- DfE (2015) 'Keeping Children Safe in Education'

This policy will be reviewed and updated in phases as the DUAA provisions come into force. We will monitor Information Commissioner's guidance and adjust accordingly.

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 (or Unique Pupil 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.

The data controller
Our federation processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller. Both federation schools are registered as a data controller with the Information Commissioner and renew this registration annually or as otherwise legally required.

The Information Asset Owners (IAO) for the federation are the Executive Headteacher and governing board.

Roles and responsibilities
This policy applies to **all staff** employed by our federation, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action. In addition, any member of staff who reports another member of staff violating the data protection principles is protected by the federation's Whistleblowing Policy.

Governing board
The governing board has overall responsibility for ensuring that our federation complies with all relevant data protection obligations. The governor with responsibility for data protection compliance is Mrs Rosie Hoyle. Data protection is an agenda item at every full governors meeting, so the federation's compliance can be reviewed.

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

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

Our DPO is Mr Tim Pinto from The E-Safety Office Ltd and is contactable via either federation school office.

Executive Headteacher
The Executive Headteacher acts as the representative of the data controller on a day-to-day basis. Some of the tasks related to this may be delegated to other members of staff.

All staff
Staff are responsible for:

- collecting, storing and processing any personal data in accordance with this policy
- informing the federation of any changes to their personal data, such as a change of address
- contacting the DPO in the following circumstances:
    - with any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - if they have any concerns that this policy is not being followed
    - if they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - if they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data to a 'third country;'
    - 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.

Data protection principles

The UK-GDPR is based on data protection principles that our federation must comply with. The principles say that personal data must be:

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

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

Collecting personal data

Lawfulness, fairness and transparency

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

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

- the individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent.**

For special categories of personal data, we also meet one of the special category conditions for processing which are set out in the UK-GDPR and Data Protection Act 2018.

The federation uses a number of online services to support the teaching and learning and safeguarding of children in the federation. This falls under the legitimate interests of processing, however some services do need explicit consent and we contact parents directly.

We may use some services where the parent has to register their details with a third-party company e.g. catering services. On these occasions, the federation highlights the privacy notice of the third-party company.

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

In addition to existing lawful basis (such as consent, legitimate interests), we may make use of the new lawful basis of recognised legitimate interests (Article 6(1)(ea)) for certain processing (e.g., safeguarding, security, emergency response). Where this is adopted, we will document the rationale and apply appropriate safeguards.

Limitation, minimisation and accuracy
We only collect personal data for specified, explicit and legitimate reasons. We 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 inform the individuals concerned before we do so, and seek consent where necessary.

Staff 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 ensure it is deleted or anonymised. This is done via secure manner using a secure confidential waste bin. Any destruction of a large amount of data is logged by the data protection lead in the federation.

Paper data that has to be retained for a specific period of time, is kept in an archived area which has restricted access. Only specific staff are allowed access to this area.

In addition, staff follow the retention schedule for electronic data and ensure that they use a file system to ensure that data can be easily accessed.

This is done in accordance with the Information and Records Management Society's toolkit for schools.

We maintain up-to-date records of processing activities, DPIAs, risk assessments, and algorithmic governance documentation, incorporating the changes introduced by the Data (Use and Access) Act.

Sharing personal data

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

- there is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- we need to liaise with other agencies - we 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:
    - only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We 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.

As the UK is now classed as a 'third country' it will ensure that it obtains a Standard Contractual Contract with data processed outside the European Economic Area.

When transferring personal data outside the UK, we ensure that protections equivalent to or not materially lower than UK standards apply, using safeguards such as standard contractual clauses, binding corporate rules, or other mechanisms.

Subject access requests and other rights of individuals

Subject access requests

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

- confirmation that their personal data is being processed
- access to a copy of the data
- the purposes of the data processing

- the categories of personal data concerned
- who the data has been, or will be, shared with
- how long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- the source of the data, if not the individual
- whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject access requests must be submitted in writing, either by letter, email or fax to the federation. They can also be made by the federation's Social Media account. It is important to note that during the summer holidays, all post is held by Royal Mail so all SARs should be made by email. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested.

In some circumstances, the federation may ask the data subject to show identification to verify their relationship with a pupil.

If staff receive a subject access request, they must immediately forward it to the Executive Headteacher.

Children and subject access requests

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

Children below the age of 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 federation 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

When responding to requests, we:

- may ask the individual to provide 2 forms of identification
- may contact the individual via phone to confirm the request was made
- will respond without delay and within 1 month of receipt of the request
- will provide the information free of charge
- may tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if it:

- might cause serious harm to the physical or mental health of the pupil or another individual
- would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- is contained in adoption or parental order records
- is given to a court in proceedings concerning the child.

We carry out a reasonable and proportionate search for personal data when responding to a subject access request. If we require clarification or additional information to process a request, we may pause the response time until such clarification is received.

If the request is unfounded or excessive, we may refuse to act on it or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

Individuals wishing to make a complaint about how we handle their personal data should submit it to Mrs Cheryl Baxter. We will acknowledge the complaint within 30 calendar days and respond without undue delay. If the complainant remains dissatisfied, they may escalate the matter to the Information Commissioner.

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, 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 a third country
- object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- prevent processing that is likely to cause damage or distress
- be notified of a data breach in certain circumstances
- make a complaint to the ICO
- ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO (through either federation school office). If staff receive such a request, they must immediately forward it to the DPO.

Parental requests to see the educational record

Parents, or those with parental responsibility, may have access to their child's educational record (which includes most information about a pupil that the federation holds on the MIS system) within 15 school days of receipt of a written request.

Photographs and videos

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

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

Uses may include:

- within school on notice boards and in federation brochures, newsletters, etc.
- outside of school by external agencies such as the school photographer, newspapers, campaigns
- online on our federation website
- educational Apps *
- social media pages *
- video sharing platforms. *

* Please note that these are third party platforms and if images are shared, parents are directed to their specific private policies.

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

When using photographs and videos in this way we do not accompany them with their names. See our E-Safety Policy for more information on our use of photographs and videos.

Data protection by design and default

We 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
- completing privacy impact assessments where the federation's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO advises 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 also keep a record of attendance

- regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- maintaining records of our processing activities, including:
    - for the benefit of data subjects, making available the name and contact details of our federation schools 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.

Data security

We 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:

- passwords that are at least 3 random words containing letters and numbers are used to access federation computers, laptops and other electronic devices
- staff remote access to the federation's network from a school's device is via an encrypted private network (VPN)
- 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
- where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected
- please see the Information Security Policy for further details.

Artificial Intelligence

The federation recognises that Artificial Intelligence (AI) tools may be used to support administrative, educational and operational activities. Any use of AI involving personal data will be lawful, transparent and proportionate, and will comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and the Data Access & Use Act 2025. Staff, governors and volunteers must not input personal data, special category data or confidential information about pupils, parents, staff or the federation into AI systems unless the tool has been formally approved, appropriate contractual safeguards are in place, and a Data Protection Impact Assessment (DPIA) has been completed where required.

AI must not be used for automated decision making about pupils or staff where such decisions produce legal or similarly significant effects, unless explicitly permitted by law and subject to appropriate human oversight. The federation ensures that AI use supports safeguarding, data minimisation and security principles, and that all users receive appropriate guidance and training on the responsible and ethical use of AI.

Personal data breaches

The federation makes all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set

out in the data breach policy. When appropriate, we will report the data breach to the ICO within 72 hours. We will also report the data breach to the governing board.

Safeguarding

The federation understands that the UK-GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

The federation ensures that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- whether data was shared
- what data was shared
- with whom data was shared
- for what reason data was shared
- where a decision has been made not to seek consent from the data subject or their parent
- the reason that consent has not been sought, where appropriate.

When providing online services that pupils are likely to access, we consider and apply measures to protect children's data rights, and limit processing to what is appropriate given their lesser awareness of risks.

The federation aims to gain consent to share information where appropriate; however, will not endeavour to gain consent if to do so would place a child at risk. The federation will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

DBS Data

All data provided by the DBS is handled in line with data protection legislation; this includes electronic communication. Data provided by the DBS is never duplicated. Any third parties who access DBS information are made aware of the data protection legislation, as well as their responsibilities as a data handler.

Training

All staff and governors are provided with data protection training as part of their induction process. Data protection also forms part of continuing professional development, where changes to legislation, guidance or the federation's processes make it necessary.

Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed and updated when any changes take place to data protection law. Otherwise, or from then on, this policy will be reviewed **every 2 years** and shared with the full governing board.