Whinless Down Academy Trust

Data Protection Policy

Spring 2022

Whinless Down Academy Trust
Data Protection Policy

Policy

Aims

This policy applies to all members of staff at Whinless Down Academy Trust. For the purposes of this policy the term 'staff' means all members of staff within the Trust, including permanent, fixed term and temporary staff. It also refers to governors, any third-party representatives, agency workers, volunteers, interns, agents and sponsors engaged with the Trust.

Our Trust 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 Data Protection Act 2018 and the General Protection Regulation (GDPR)

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the GDPR personal information, also includes an identifier such as a name, an identification number, location data or an online identifier.

Each school collects a large amount of personal data every year, including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the schools. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

Policy Objectives

Each school and the Trust as Data Controllers will comply with its obligations under the GDPR and DPA. The Trust is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

Legislation and guidance

This policy meets the requirements of the GDPR and the provision of the DPA 2018. It is based on guidance published by the Information Commissioners Office (ICO) on the GDPR and the ICO's code of practice for subject assess requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

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 education record.

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

Trustees
The board of Trustees and its Local Governing Bodies have overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

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.

Our DPO is Mike Ashley and is contactable via the Trust governance professional p.a.toheadteacher@prioryfields.kent.sch.uk

Head Teacher
The head Teacher in each school within the Trust acts as the representative of the data controller on a day-to-day basis.

All Staff
Staff are responsible for;

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the school of any changes to their personal data, such as a change of address.
- Contacting the Head Teacher who will contact the Trust Business Manager 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 there has been a personal data breach or a cyber-security incident in which there is potential for a personal data breach to occur.
    - In circumstances where a notification may need to be made to the Information Commissioner's Office.
    -

Individual Responsibilities
During their employment, staff may have access to the personal information of other members of staff, suppliers, clients or the public. The school expects staff to help meet its data protection obligations to those individuals.

If you have access to personal information, you must:

- only access the personal information that you have authority to access and only for authorised purposes
- only allow other staff to access personal information if they have appropriate authorisation
- only allow individuals who are not school staff to access personal information if you have specific authority to do so
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction in accordance with the school's policies).
- not remove personal information, or devices containing personal information (or which can be used to access it) from the school's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device
- not store personal information on local drives or on personal devices that are used for work purposes.

Data Protection principles

The GDPR is based on data protection principles that our Trust and its schools must comply with. The principles set out in the GDPR must be adhered to when processing personal data:

1. Personal data must be processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
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**)
3. Personal data shall be adequate, relevant and limited to what is necessary in relation to the purpose(s) for which they are processed (**data minimisation**)
4. Personal data shall be accurate and where necessary kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay (**accuracy**).
5. Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data is processed (**storage limitation**)
6. Appropriate technical and organisational measures shall be taken to safeguard the rights and freedoms of the data subject and to ensure that personal information are processed in a manner that ensures appropriate security of the personal data and protects against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**).

Process

Collecting personal data

Lawfulness, fairness and transparency

Before any processing activity starts for the first time and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected.
We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law;

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party[1]
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interest's assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information
Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or are genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
    (a) the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
    (b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
    (c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
    (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
    (e) the processing relates to personal data which are manifestly made public by the data subject
    (f) the processing is necessary for the establishment, exercise or defence of legal claims
    (g) the processing is necessary for reasons of substantial public interest
    (h) the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
    (i) the processing is necessary for reasons of public interest in the area of public health.

Each school within the academy's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the GDPR.

Data Protection Impact Assessments (DPIA)
All data controllers are required to implement 'Privacy by Design' when processing personal data. This means the Academy Trust's processes must embed privacy considerations and incorporate appropriate technical and organisational measures (like pseudonymisation) in an effective manner to ensure compliance with data privacy principles.

Where processing is likely to result in high risk to an individual's data protection rights (for example where a new technology is being implemented) a DPIA must be carried out to assess:

- whether the processing is necessary and proportionate in relation to its purpose
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Staff should adhere to the Data Protection Toolkit for Schools from the DfE with reference to the DPIA template.

When carrying out a DPIA, staff should seek the advice of the DPO for support and guidance and once complete, refer the finalised document to the DPO for sign off.

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 schools holds about them. This includes;

- Confirmation that their personal data is being processed.
- Access to a copy of the data.
- The purpose 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 is not 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 head teacher of the school. They should include;

- Name of individual
- Correspondence address
- Details of information requested.

If staff receive a subject access request, they must immediately forward it to the Head Teacher. The Head Teacher must keep a record of the requests received and forward the details to the Trust Business Manager who will forward it to the DPO to enable the Trust's DPO to have oversight of the process being completed.

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 onerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

We will not disclose information if;

- 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 orders records.
- Is given to a court in proceedings concerning the child.

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

When we refuse a request we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

Staff, as well as any other 'data subjects', have the following rights in relation to their personal information:

- To be informed about how, why and on what basis that information is processed *(see the relevant privacy notice)*
- To obtain confirmation that personal information is being processed and to obtain access to it and certain other information, by making a subject access request *(see Protocol for Access to Personal Information)*
- To have data corrected if it is inaccurate or incomplete
- To have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing ('the right to be forgotten')
- To restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased) or where the school no longer need the personal information, but you require the data to establish, exercise or defend a legal claim
- To restrict the processing of personal information temporarily where you do not think it is accurate (and the school are verifying whether it is accurate), or where you have objected to the processing (and the school are considering whether the school's legitimate grounds override your interests)
- In limited circumstances to receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format
- To withdraw consent to processing at any time (if applicable)
- To object to decisions based solely on automated processing, including profiling
- To be notified of a data breach which is likely to result in high risk to their rights and obligations
- To make a complaint to the ICO or a Court.

Biometric recognition systems
The Trust currently does not use Biometric systems

CCTV
We use CCTV in various locations around the Trust school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Photographs and videos
As part of our school activities, we may take photographs and record images of individuals within our schools.
We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to the parent/carer.

Uses may include;

- Within school on notice boards, school magazines, brochures, prospectus etc.
- Outside of school by external agencies such as the school photographer, newspapers, projects, sports events etc.
- 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 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.

Documentation and records
We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosures 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. If the laptop is taken home for use by staff member, the staff member will ensure that the laptop is stored securely 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.
- Personal information should not be taken off site except in exceptional circumstances and then permission needs to be granted by the TBM, CEO or HT.
- Passwords are at least 8 characters long containing numbers and letters to access school computers, laptops and other electronic devices. Password systems ensure that passwords are changed on staff devices. (See Password Policy)
- Encryption software is used to protect all portable devices and pen drives, such as laptops and USB devices.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is store securely and adequately protected.

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, whether we cannot or do not need to rectify or update it. Disposal will be through shredding paper-based records and overwriting or deleting electronic files. We may also use a third party to safely dispose of records on the school's behalf and overseen by school staff. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Storage and retention of personal information
Personal data will be kept securely in accordance with the school's data protection obligations.
Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the KCC Information Management Toolkit for Schools on KELSI with reference to the Record Retention Schedule, available at the following link:
http://www.kelsi.org.uk/__data/assets/word_doc/0012/60213/InformationManagementToolkitforSchoolsv4-2.docx

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

Data minimisation
Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Staff may only process data when their role requires it. Staff must not process personal data for any reason unrelated to their role.

The School maintains a Retention Schedule to ensure personal data is deleted after a reasonable time for the purpose for which it was being held, unless a law requires such data to be kept for a minimum time. Staff must take all reasonable steps to destroy or delete all personal data that is held in its systems when it is no longer required in accordance with the Schedule. This includes requiring third parties to delete such data where applicable.

Privacy Notice
The Academy Trust will issue privacy notices as required, informing data subjects (or their parents, depending on age of the pupil, if about pupil information) about the personal information that it collects and holds relating to individual data subjects, how individuals can expect their personal information to be used and for what purposes.

Each school within the Academy Trust will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Information Security
The Trust will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable use policy.

The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

Availability means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

Data breaches
A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

All data breaches must be reported to the Trust Business manager immediately who must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the Academy Trust's agreed breach reporting process.

Training
The Academy Trust will ensure that all staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the Trust and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or your school's DPO.

The DPO for the Whinless Down Academy Trust is Mike Ashley. He can be contacted through the Governance Professional at: p.a.toheadteacher@prioryfields.kent.sch.uk

Review of Policy
This policy will be updated Spring 2025 to reflect best practice or when ther are amendments made to the GDPR or DPA.

The Supervisory Authority in the UK
Please follow this link to the ICO's website (https://ico.org.uk/) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.