Data Protection Policy

Adoption Arrangements

All statutory policies in the Trust are ultimately the responsibility of the Trust Board. To enable it to discharge this responsibility appropriately and in collaboration with the constituent schools, the Trust Board will

1. set a full Trust wide policy,
2. set a 'policy principles' document (a framework within which Headteachers develop a full and appropriately customised policy),
3. or delegate to Headteachers or LGBs the power to develop their own policy.

Approval Body:	**Board of Trustees**
Adopted:	**7 July 2022**
Leadership Grp Responsibility:	**Data Protection Officer**
Review period:	**Annual**
Date of next review:	**July 2023**

This is a Level 1 Policy against the Trust Governance Plan.

This policy was adopted by the Trust Board, for implementation in Tenax Schools Trust on the date above and supercedes any previous policy on data protection.

Appendix 1: Data Breach Procedure
Appendix2: Keeping Data Safe
Appendix 3: Legal conditions for processing

Introduction

Our Data Protection Policy lays out the approach for Tenax Schools Trust, as the Data Controller, to data protection. We recognise the importance of protecting the personal data we are entrusted with, and this policy sets out how we comply with relevant 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.

If you have any queries about this Policy, please contact our Data Protection Officer, Catherine Dottridge (contact details on page 2)

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

All staff are responsible for reading and understanding this policy before carrying out tasks that involve collecting or handling personal data, and for following this policy, including reporting any suspected data breaches, any subject access requests or Freedom of Information requests to our Data Protection Officer. All leaders are responsible for ensuring their team read and understand this policy before carrying out tasks that involve collecting or handling personal data, and that they follow this policy.

There are separate policies covering: Records Management Policy, Records Retention Schedule and a Freedom of Information Publication Scheme. These are available on the Tenax Schools Trust website https://www.tenaxschoolstrust.co.uk/.

Data Protection Officer (DPO)

A DPO must be appointed in order to:

- Inform and advise the Trust and its employees about their obligations to comply with the data protection laws.
- Monitor the Trust's compliance with the data protection laws, including managing internal data protection activities, advising on data protection impact assessments, and providing the required training to staff members.
- Act as a contact point for data subjects and the supervisory authority

The Trust Board has appointed Mrs Catherine Dottridge as the Trust's DPO:

Mrs C Dottridge, Chief Finance Officer, Tenax Schools Trust c/o Bennett Memorial Diocesan School, Culverden Down, Tunbridge Wells, TN4 9SH. Telephone: 01892 521595

DPO@tenaxschoolstrust.co.uk

The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

The school will issue privacy notices as required, informing data subjects (or their parents/legal guardian 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.

The school will issue a minimum of two privacy notices, one for pupil information, and one for workforce information, and these will be reviewed in line with any statutory or contractual changes. Current versions are available on the school and Trust website.

The right of access (Subject Access Requests)

Individuals have the right to obtain confirmation that their data is being processed. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data.

The Trust will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, we will normally provide this information electronically in a secure format (password protected PDF sent via email) unless the individual requests otherwise.

We will respond to, and fulfil, all valid requests within one calendar month, unless it is necessary to extend the timescale, by up to two months in certain circumstances. Not all the rights are absolute rights, and we cannot always carry out the requested action in full, or at all. For example, a number of exemptions in the DPA 2018 apply to SARs, meaning we can withhold some information in some situations. In responding to requests, we also explain to data subjects they have the right to make a complaint to the ICO.

In the event that a large quantity of information is being processed about an individual, the Trust will ask the individual to specify the information the request is in relation to.

We may refuse to provide all or part of the information requested if an exemption or restriction applies, or if the request is manifestly unfounded or excessive.

Before responding to a SAR for information held about a child, we will consider whether the child is mature enough to understand their rights. If the request is from a child and we are confident they can understand their rights, we will usually respond directly to the child. We may, however, allow the parent or legal guardian to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child. If a child is competent, they may authorise someone else, other than a parent or guardian, to make a SAR on their behalf.

<u>If the school receives a SAR, the Headteacher and DPO must be informed.</u>

Freedom of Information requests

Information held by an academy that is not published under the Tenax School's Trust Freedom of Information Publication Scheme can be requested in writing from the Headteacher of the individual school, or from the DPO, when its provision will be considered in accordance with the provisions of the Freedom of Information Act 2000.

If the school receives a Freedom of Information request, the Headteacher and DPO must be informed.

Individual Responsibilities

During their employment, staff may have access to the personal information of pupils and students, parents and carers, other members of staff, suppliers, clients or the public. The school expects staff (and volunteers) to help meet its data protection obligations to those individuals.

Staff with access to personal information, must follow the "Keeping data safe" guidance in Appendix 2.

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

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

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 Records Management Policy and Records Retention Schedule.

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 data protection laws.

Contracts with external organisations

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 should seek approval from the DPO.

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 school's Records Management Policy and the Record Retention Schedule, both available via the school office.

Personal information that is no longer required must be deleted and/or securely destroyed in accordance with the Records Management Policy.

Data Breaches

Staff must inform their Headteacher and DPO immediately that a data breach is discovered and make all reasonable efforts to recover the information. Staff should refer to the school's breach procedure below. The school must report a significant data breach via the DPO 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.

Training

The school will ensure that 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 school 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 where proven, this action may result in sanctions up to 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 Headteacher or the DPO.

Implementation

The Headteacher/DPO should ensure that staff are aware of the school's Data Protection policy and its requirements including the data breach procedure. This should be undertaken as part of induction and ongoing training. If staff have any queries in relation to the school's Data Protection policy and associated procedures, they should discuss this with their line manager, Headteacher or the DPO.

Review of Policy

This policy will be reviewed every year, or updated as necessary to reflect best practice or amendments made to relevant legislation.

Appendix 1: **Data Breach Procedure**

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

Loss or theft of pupil, staff or governing body data and/ or equipment on which data is stored;
Inappropriate access controls allowing unauthorised use;
Equipment Failure;
Poor data destruction procedures;
Human Error;
Cyber-attack;
Hacking.

Managing a Data Breach

In the event that the school identifies or is notified of a personal data breach, the following steps are to be followed:

1. The person who discovers/receives a report of a breach must inform the Headteacher or, in their absence the Deputy Headteacher, and the Data Protection Officer (DPO). If the breach occurs or is discovered outside normal working hours, this reporting should begin as soon as is practicable.

2. The Headteacher and DPO (or nominated representative(s)) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.

4. The Headteacher and DPO (or nominated representative (s)) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

5. The Headteacher/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

a. Attempting to recover lost equipment.
b. The use of back-ups to restore lost/damaged/stolen data.
c. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
d. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the members of staff informed.

Investigation

In most cases, the next stage would be for the Headteacher/DPO (or nominated representative) to fully investigate the breach. The Headteacher/DPO (or nominated representative) should ascertain whose data

was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

The type of data;
Its sensitivity;
What protections were in place (e.g. encryption);
What has happened to the data;
Whether the data could be put to any illegal or inappropriate use;
How many people are affected;
What type of people have been affected (pupils, staff members, suppliers etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The Headteacher/DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what the school is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (via the School's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the Headteacher/DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with the Trust's HR Director for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

We will log all breaches centrally, including those not reportable to the ICO.

Appendix 2: **Keeping Data Safe**

All staff, Governors and volunteers are personally responsible for the day-to-day security of any personal or sensitive data you use.

1. You **must** make sure you **follow security rules**. Don't bypass security software for any reason or take chances with weak passwords, because they're easier to remember.
2. Always make sure you **dispose of papers** containing personal information – either in confidential waste bins or **by shredding**. NEVER throw them away in the normal waste paper basket or put them into recycling.
3. If you deal with sensitive or personal data, try to **adopt a clear desk policy**, which means making sure you don't leave information which is sensitive or personal on your desk, on the printer or on the photocopier and lock papers away before leaving, storing the keys safely. If data is particularly sensitive you should **lock away papers**.
4. **Turn off or lock your computer screen** when you're away from your desk, even for a short time. And be very careful that no one can read the information from your computer screen while you're working.
5. Ideally **use the secure school network** for accessing/editing personal data only – if data is needed to be saved on removable storage or a portable device, make sure the device is kept in a locked filing cabinet, drawer or safe when not in use. **Memory sticks must** not be used to hold personal information unless they are password-protected and **fully encrypted**.
6. Security includes keeping personal **data safe in transit too** – for example not leaving laptops or personal files visible in parked cars.
7. It's a good idea to **password protect personal data and files**.
8. Use **school email addresses for school business only** – and do not use personal emails for any school business.
9. Keep personal data **anonymous** where possible and **don't name the child if you don't need to** – especially in titles of emails
10. It's really important that you **stay vigilant to any attempts to compromise YOU**.
11. **Do not give your login or password details to anyone**.
12. You must ALWAYS **follow proper procedures and security checks to identify callers**. You could be prosecuted even if you unintentionally give out personal data without permission.
13. It's also important that you're careful when you're working, to not accidentally pass on anyone's personal information. For example, double-check posted **documents or electronic information are correctly addressed to the right person** and check when sending information by electronic communications, that **the recipient(s) have the right and are authorised to receive all the information** contained in the communication – otherwise delete/remove unauthorised content accordingly.
14. **Think before you send** or **put up information up on a wall** as to who really needs the data or information; and is there a safeguarding risk in displaying it - being particularly careful about the use of group emails or displaying information in public places.
15. Any **circular emails to parents must be sent blind carbon copy (bcc),** so personal email addresses are not disclosed to other recipients.
16. Be careful that you **don't disclose someone's personal details by letting something slip** to someone who doesn't have a right to know it.

Loss of personal data is a very serious breach of security.

If you think there's been a breach of security, never try to cover it up or hide it. Always report it straight away to the Headteacher and the Trust's Data Protection Officer, Catherine Dottridge.

Remember that data protection laws DO NOT stop you from reporting safeguarding concerns.
You must still report to the relevant people where you're concerned about a child.

Appendix 3: **Legal conditions for processing**

Definitions

"Personal data" means any information where a living person is either identified or identifiable, from the information alone, or with other information. Personal data can include written information, pupil work, photographs, CCTV and film footage or voice recordings, in electronic format (which can include in social media, apps, databases or other electronic formats) or hard copy (including copies printed from electronic sources, and handwritten data when it is part of a filing system or intended to be filed).

"Special category data" is personal data that needs more protection because it is sensitive. • personal data revealing racial or ethnic origin • personal data revealing political opinions • personal data revealing religious or philosophical beliefs • personal data revealing trade union membership • genetic data • biometric data (where used for identification purposes) • data concerning health • data concerning a person's sex life • data concerning a person's sexual orientation • In addition, the DfE advises that Pupil Premium/FSM status is treated as Sensitive Data.

"Data Subjects" include our pupils, staff, contractors, parents, local authority contacts, and anyone else we might come into contact with.

"Data Controller" means the Tenax School's Trust, decides on why and how personal data is processed.

"Processing" means collecting, storing, using, sharing and disposing of data.

"Processors" are the external bodies who processes personal data on behalf of the controller

The Principles

In accordance with the legislation, personal data will be:

1. Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**)
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**)
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**)
4. Accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**accuracy**)
5. 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. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**).

The GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

Transfer Limitation

In addition, personal data will not be transferred to a country outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Staff should contact the DPO if they require further assistance with a proposed transfer of personal data outside of the EEA.

Lawful Processing

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained

- Processing is necessary for:
  - Compliance with a legal obligation
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party

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 should be identified and documented.

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

Consent

Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

Where consent is given, a record will be kept documenting how and when consent was given.

Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

Consent can be withdrawn by the individual at any time.