THAMESVIEW SCHOOL

Thong Lane, Gravesend, Kent DA12 4LF

Data Policy

THAMESVIEW SCHOOL
DATA POLICY

The General Data Protection Regulations (GDPR) superseded the Data Protection Act 1998 and is the law that protects personal privacy and upholds individual's rights.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 GDPR. It will apply to information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

The legal bases for processing data are as follows –
(a) Consent: the member of staff/student/parent has given clear consent for the school to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.
(c) Legal obligation: the processing is necessary for the school to comply with the law (not including contractual obligations)

All staff must treat all student information in a confidential manner and follow the guidelines as set out in this document. The school is also committed to ensuring that its staff are aware of data protection policies, legal requirements and adequate training is provided to them through online training and other appropriate CPD. The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Scope of the Policy

Personal information is;
'*Any information relating to an identifiable natural person' (data subject)*
'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identify of that natural person.'

Article 4(1) of the GDPR

The School collects a large amount of personal data every year including, but not exclusive to: 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 School. 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.

Responsibilities

The school must:

- Manage and process personal data properly
- Protect the individual's right to privacy
- Provide an individual with access to all personal data held on them.

The school has a legal responsibility to comply with the Act. The school, as a corporate body, is named as the Data Controller under the Act.

Data Controllers are people or organisations who hold and use personal information. They decide how and why the information is used and have a responsibility to establish workplace practices and policies that are in line with the Act.

The school is required to 'notify' the Information Commissioner of the processing of personal data. This information will be included in a public register which is available on the Information Commissioner's website at the following address https://ico.org.uk/

Every member of staff that holds personal information has to comply with the Act when managing that information.

The school is committed to maintaining data security at all times. This means that the school will:

- inform Data Subjects why they need their personal information, how they will use it and with whom it may be shared. This is known as a Privacy Notice.
- check the quality and accuracy of the information held
- apply the records management policies and procedures to ensure that information is not held longer than is necessary
- ensure that when information is authorised for disposal it is done appropriately
- ensure appropriate security measures are in place to safeguard personal information whether that is held in paper files or on a computer system
- only share personal information with others when it is necessary and legally appropriate to do so
- set out clear procedures for responding to requests for access to personal information known as subject access requests ***(see appendix)***
- train all staff so that they are aware of their responsibilities and of the schools relevant policies and procedures

Please follow this link to the ICO's website (www.ico.org.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. In particular, you may find it helpful to read the Guide to Data Protection which is available from the website.

For help or advice on any data protection or freedom of information issues, please write to;

Information Resilience and Transparency Team, Kent County Council, Room 2.71, Sessions House, County Hall, Maidstone. ME14 1XQ

Fax: 03000 420303
Email: freedomofinformation@kent.gov.uk

Reporting a data breach

Data breaches are any incidents where personal information has been wrongly shared by the controller. An example of this could be where a sensitive email has been sent to the wrong address and it contained personal information about staff or students. Another example could be where a USB drive has been lost or stolen which contained sensitive data. If this happens staff are to report this to the Data Protection Lead in school who will then log this as a breach in the online school log. The Data Protection Lead will inform the ICO within 72 hours, and inform the individual(s) that are affected by the breach.

Staff are required to report data breaches as this helps the school review procedures, and failure to report a breach could make the situation worse.

Privacy notices.

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.
There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, Ofsted, or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.
The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information. Any proposed change to the processing of individual's data shall first be notified to them.

Privacy notices will be provided on the school website and will be on display in the following places;
Student and parent privacy notice- Main reception
Staff privacy notice- Staff room

Security.

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Staff will ensure the security of data in the following ways;

1. Passwords for access to technical systems, including online accounts, will not be shared with others, written down and kept with devices and will be changed as requested.

2. Laptops will be put into 'lock' mode when unattended so that others cannot access data on their devices.
3. All external drives such as USB drives will be encrypted so that data is kept secure.
4. Report any loss or theft of external devices used for work purposes, as well as the loss or theft of laptops, mobile devices and tablets.
5. Register with the ICT technicians that they are using school emails on their personal phones.
6. If school emails are being used on personal devices staff will;
    a. Ensure that the device has a lock on it (password/ biometric) and not share this.
    b. Not share emails with anyone who is not a member of school staff.
    c. When selling or disposing of the device all data should be removed.
7. When taking paperwork home (marking, administration work or student work) staff will take all reasonable precautions to ensure the data is safe i.e. not leave it in a car, or sharing it with others.
8. If the school is asked for personal data the person's identification will be requested to check for verification. This could include asking for the child's DoB plus another piece of data such as address or home phone number.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.
It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:
Hard copy data, records, and personal information of staff are stored out of sight and in a locked filing cabinet in a locked room.
Student data and information is, as far as is possible, stored on the school MIS (SIMS). Paper copies of information are scanned onto the MIS and then disposed of as confidential waste.

Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:
• Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.

• Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.

• Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

• If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

• If it is necessary to transport data away from the school, it should be downloaded onto a USB stick. The data should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB only.

- If staff are using the VPN to access data from school this must not be copied onto the personal computer, and all editing and work must be done through the VPN connection.

• USB sticks that staff use must be password protected.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:
The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance.

Reviewing:
This guide and policy will be reviewed, and updated if necessary every year.

DATA POLICY

This Policy was agreed and adopted at a Governors' meeting held on _____ (date)

Signed_____ (Governor)

Signed_____ (Headteacher)

This policy will be formally reviewed in _____ (date)

APPENDIX 1

Data Access Requests (Subject Access Requests):
All individuals whose data is held by us, has a legal right to request access to such data or information about what is held.
We shall respond to such requests within one month and they should be made in writing to:

Headteacher
Thamesview School
Thong Lane
Gravesend
Kent
DA12 4LF

No charge will be applied to process the request.

Personal data about pupils will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

• Other schools If a pupil transfers from Thamesview School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

• Examination authorities This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.

• Health authorities As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.

• Police and courts If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

• Social workers and support agencies In order to protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

• Educational Authorities; Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

• Right to be forgotten: Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the school including any data held by contracted processors

In addition to this the school will;

1. Keep the original request and note against this who dealt with the request and when the information was provided.

2. Ensure that any data requested and given over in a Subject Access Request is signed for and a log is kept of the request details (such as date requested, date given etc).

3. Any complaint about the provision of information will be handled by the Head Teacher or another senior member of staff. All complaints should be in writing and documented. The Publication Scheme will include information on who to contact for both enquiries and complaints.

4. All enquirers should be advised that they may complain to the information Commissioner if they are unhappy with the way their request has been handled.