# Data Protection Policy

# 2025 - 2026

| | |
|---|---|
| **Version** | 1 – Supersedes all previous policies |
| **Document authors** | Mr. S. Proctor |
| **Other contributors** | IGS |
| **Policy approved (date)** | October 2025 |
| **Policy to be reviewed (date)** | October 2026 |
| **Other related policies** | Data Breach Policy<br>Data Handling Security Policy<br>Acceptable Personal Use Policy<br>Statutory Request Policy<br>Privacy Notice<br>Complaints Policy<br>Whistleblowing Policy |

## Purpose of Policy

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

## Roles within the school

Data Protection Officer (DPO) - IGS - Information Governance Support

Senior Information Risk Owner (SIRO) - Mr. S. Proctor

Information Champion (IC) - Mrs. J. Pitcher

Information Governance Governor - Mrs. S. Stronach

Data protection is a legal requirement and is vitally important for ensuring that the data of our students, parents/carers, and those that work with the school is kept secure. This will protect the rights of individuals and ensure that the risks of data processing are well managed.

This policy sets out the rules all staff, governors, contractors and volunteers **must** follow when processing personal data.

## Policy rules:

1. All employees must **comply** with the requirements of Data Protection Law and Article 8 of the Human Rights Act when processing the personal data of living individuals.
2. Where personal data is used, we must make sure that the data subjects have access to a complete and current **Privacy Notice.**
3. We must formally **assess** the risk to privacy rights introduced by any new (or change to an existing) system or process which involves the use of personal data, by completing a **Data Protection Impact Assessment (DPIA)**.
4. We must process only the **minimum** amount of personal data necessary to deliver services.
5. All employees who record **opinions** or intentions about students, parents/carers or staff must do so carefully and professionally, distinguishing between fact and opinion.
6. We must take reasonable steps to ensure the personal data we hold is **accurate**, up to date and not misleading.
7. We must rely on **consent** as a condition for processing personal data only if there is no relevant legal power or other condition.
8. Consent must be obtained if personal data is to be used for **promoting or marketing** goods and services, unless you have statutory duties to promote them.
9. Consent will **expire** at the end of each 'Key Stage' period unless it is reconfirmed.
10. We must ensure that the personal data we process is reviewed and **destroyed** when it is no longer necessary.
11. If we receive a **request** from a member of the public or colleague asking to receive a copy of their personal data, we must handle it as a Subject Access Request under the Data Protection Act 2018 or a request for the Education Record under the Education (Pupil Information) (England) Regulations 2005.
12. If we receive a request from anyone asking to access the personal data of **someone other than themselves**, we must fully consider Data Protection law before disclosing it.
13. When someone contacts us requesting we change the way we are processing their personal data, we must fully consider their **rights** under Data Protection law.

14. You must not access personal data which you have **no right to view.**
15. You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so.
16. You must only **share** personal data with external bodies who request it if there is a current agreement in place to do so or it is approved by the Data Protection Officer (DPO) or Senior Information Rick Owner (SIRO).
17. Where the content of telephone calls, emails, internet activity and video images of employees and the public is **recorded, monitored and disclosed** this must be done in compliance with the law and the regulator's Code of Practice.
18. All employees must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely. This training must be regularly refreshed to ensure knowledge remains current.
19. When using **'data matching'** techniques, this must only be done for specific purposes in line with formal codes of practice, informing students, parents/carers or staff of the details, their legal rights and getting their consent where appropriate.
20. We must pay an annual Data Protection Fee.
21. Where personal data needs to be anonymised or pseudonymised, for example for **research purposes**, we must follow the relevant procedure.
22. You must not **share** any personal data held by us with an individual or organisation based in any country outside of the United Kingdom without seeking advice from the SIRO or DPO.
23. We must identify **Special Categories** of personal data and make sure it is handled with appropriate security and only accessible to authorised persons.
24. When **sending** Special Category data to an external person or organisation, it should be marked as "OFFICIAL-SENSITIVE" and where possible, sent by a secure method.
25. When considering the use of **artificial intelligence** involving the using or creation of personal data you can only do so on approval from the DPO.

## How must I comply with these policy rules?

We have related policies, procedures and guidance which tell you how to comply with these rules. These include:

- Statutory Requests Policy
- Data Handling Security Policy
- Data Breach Policy
- Records Management Policy
- Privacy Notice Procedure
- Data Protection Rights Procedure
- Publishing for Transparency Procedure

- Consent Procedure
- Minimisation of Personal Data Procedure
- Data Breach Procedure
- Data Sharing Procedure
- Subject Access Request Procedure
- Marketing Procedure
- Surveillance Procedure
- Retention Schedule
- Training & Awareness Procedure
- Statutory Requests for Information Guidance
- Overseas Transfers & Hosting Guidance

If you are unsure how to comply you must seek advice and guidance from your Data Protection Lead.

## Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator). The school's complaints policy can be found on the school's website.

## What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Mr. S. Proctor (Head Teacher - SIRO - admin@westthurrockacademy.co.uk)

If you believe the policy does not meet your business needs, you may raise this with your Information Champion who, if they agree with your suggestion, may propose a policy change.

## Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

## Contacts

If you have any enquires in relation to this policy, please contact Mr. S. Proctor (the school's Head Teacher) on 01708 866 743 or admin@westthurrockacademy.co.uk . The Head Teacher will also act as the contact point for any subject access requests.

Further advice and information is available from the Information Commissioner's Office - www.ico.gov.uk

## References

- Data Protection Act 2018 (including the UK General Data Protection Regulation)
- Article 8, The Human Rights Act 1998
- Education (Pupil Information) (England) Regulations 2005
- Investigatory Powers Act 2016
- Privacy and Electronic Communications Regulations 2003
- The Equality Act 2010