WOODLANDS SCHOOL
PURSUE EXCELLENCE & SEIZE OPPORTUNITIES

Data Protection Policy

Version 1:	June 2018
Date approved:	June 2018
Approved by:	Standards, Staffing and Curriculum
Next review:	June 2019

Woodlands School is part of Takely Education Trust, a company limited by guarantee, registered in England and Wales. Company number 9451372.
Registered Office: The Appleton School, Croft Road, Benfleet, Essex, SS7 5RN

Woodlands School collects and uses personal information about staff, pupils, parents/carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Schools also have a duty to issue a Privacy Notice to all pupils/parents. This summarises the information held on pupils, why it is held and the other parties to whom it may be passed on.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the GDPR 2016, 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.

What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

General Statement

The school is committed to maintaining the GDPR principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected.
- Inform individuals when their information is shared, and why and with whom it was shared.
- Check the quality and the accuracy of the information it holds.
- Ensure that information is not retained for longer than is necessary.
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures.

GDPR Principles

The General Data Protection Regulation establishes seven key principles relating to the processing of personal data.

1. Lawfulness, fairness and transparency - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
2. Purpose limitation - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimisation - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accuracy - Personal data shall be accurate and, where necessary, kept up to date.
5. Storage limitation - Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

6. Integrity and confidentiality - Personal data shall be 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.
7. Accountability - The controller shall be responsible for, and be able to demonstrate compliance with the GDPR.

Responsibilities

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. Refer to the privacy notice procedure for guidance.
3. We must formally assess the risk to privacy rights introduced by any new (or change to an existing) system or process which processes personal data. A privacy impact assessment must be completed and approved.
4. We must process only the minimum amount of personal data necessary to deliver services. The law states that we must only process the minimum amount of information needed to carry out our purpose.
5. All employees who record opinions or intentions about service users must do so carefully and professionally. This is to maintain professional standards, and to assist in defending the validity of such comments if the data subject exercises their rights to ask us to amend or delete their personal data if they feel it to be inaccurate.
6. We must take reasonable steps to ensure the personal data we hold is accurate, up to date and not misleading. There should be a check of the currency of data held, and whenever contact is re-established, you should check that the information you hold is still correct.
7. We must rely on consent as a condition for processing personal data only if there is no relevant legal power or other condition. Refer to consent procedure for guidance.
8. Consent must be obtained if personal data is to be used for promoting or marketing goods and services. Refer to consent procedure for guidance.
9. We must ensure that the personal data we process is reviewed and destroyed when it is no longer necessary. This links in with the records management policy. We must review personal data regularly and delete information which is no longer required; although we must take account of statutory and recommended minimum retention periods
10. If we receive a request from a member of the public or colleagues asking to access their personal data, we must handle it as a Subject Access Request. Refer to statutory requests policy for guidance.
11. 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. Refer to statutory requests policy for guidance.
12. When someone contacts us requesting we change the way we are processing their personal data, we must consider their rights under Data Protection law.
13. You must not access personal data which you have no right to view. Personal data must be protected by effective security controls to ensure only approved access. You must inform your manager if you have access to data which you are not entitled to view.
14. 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. Personal data must be protected by effective security controls to ensure that only those with approved access can view the data.
15. You must share personal data with external bodies who request it only if there is a current agreement in place to do so or it is approved by the Data Protection Officer.
16. 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. The law permits organisations to hold such data in order to measure the quality of services being provided, to record consent etc. In certain

circumstances recordings may be accessed. For further guidance refer to surveillance management procedure.

17. All employees must be trained to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
18. When using 'data matching' techniques, this must only be done for specific purposes in line with formal codes of practice, informing service users of the details, their legal rights and getting their consent where appropriate. Impact assessments must be completed and approved for the activity.
19. We must maintain an up to date entry in the Public Register of Data Controllers. This is a legal requirement and allows the public to see what personal information we hold. The entry should be reviewed annually.
20. Where personal data needs to be anonymised, for example for research purposes, we must follow the relevant procedure. Follow guidance in data minimisation procedure.
21. You must not share any personal data held by us with an individual or organisation based in any country outside of the European Economic Area. This is to ensure compliance with data protection law. Consult the data protection officer if unsure.

Complaints

Complaints about the above policy should be made to the I.E.B/Chairperson of the Governing Body who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Breach Statement

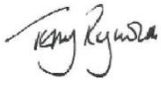
Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Contacts

If you have any queries or concerns regarding these policies/procedures then please contact Mr S Cox, Headteacher.

Signed:_____ Dated: 11th June 2018

Head Teacher



Signed:_____ Dated: 11th June 2018

Chair of Governors

Updated June 2018

PURSUE EXCELLENCE AND SEIZE OPPORTUNITIES