Wootton Academy Trust

Data Protection Policy
GDPR changes

a) This policy applies to all schools managed by Wootton Academy Trust

b) This policy was adopted by Wootton Academy Trust in 2018

c) This policy will reviewed by Wootton Academy Trust biennually

Wootton Academy Trust

Data Protection Policy

1. Introduction

To work effectively within Wootton Academy Trust, Wootton Upper School and Kimberley Sixth Form College are required to process relevant personal data about students, their parents/carers, staff and other individuals with whom the organisations have contact. Both the school and the college ('the Trust's organisations') will take all reasonable steps to do so in accordance with this policy and the principles of the European General Data Protection Regulation.

Processing means obtaining, recording or holding the information or data or carrying out any other set of operations on the information or data.
Data subject means an individual who is the subject of the personal data or the person to whom the information relates.
Personal data means data which relates to a living individual which could be used to identify the individual.
Parent has the meaning given in The Education Act (1996), and includes any person having parental responsibility or care of a child.
In this policy, any subsequent reference to students includes current, past or prospective students.

2. Obtaining further information

Further information about the Trust's Data Protection policy and procedures can be obtained from the Executive Principal. General information about the General Data Protection Regulation can be obtained from the Information Commissioner's Office (Helpline: 0303 123 1113, website: www.ico.gov.uk).

3. The principles of the General Data Protection Regulation

So far as is reasonably practicable, the Trust's organisations will comply with the principles of Article 5 of the GDPR to ensure all data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving

purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 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;
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- 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.

Article 5 (2) requires that:

- "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

4. Processing Personal Data

The Trust's organisations undertake to obtain and process data fairly and lawfully by informing all data subjects of the reasons for data collection, the purposes for which the data are held, the likely recipients of the data and the data subjects' right of access. This is included in the Privacy Notice given to data subjects.

We collect and process pupil information under Article 6 and Article 9 of the European General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect and use data under section 537A of the Education Act 1996 and section 83 of the Children's Act 1989.

We collect and process staff data under Article 6 and Article 9 of the European General Data Protection Regulation from 25 May 2018. Under Article 6(1)(e) our lawful basis for processing data is that it is a Public task and the processing is necessary for us to perform a task in the public interest. Under Article 9(2)(g) our lawful basis for processing sensitive data is that processing is necessary for reasons of substantial public interest. We also collect your data in line with section 114 of the Education Act 2005.

5. Data Integrity

The Trust's organisations undertake to ensure data integrity by the following methods:

5.1. Data Adequacy and Relevance

Data held will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Trust's organisations will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

5.2. Data Accuracy

Data held will be kept as accurate and up to date as is reasonably possible. If a data subject informs the school or college of a change of circumstances their record will be updated as soon as is practicable. A data checking sheet will be provided to data subjects according to guidance, and as quickly as is practicably possible, so they can check its accuracy and make any amendments.

5.3 Retention

Data held about individuals will not be kept for longer than necessary for the purposes registered. We hold pupil data electronically for 20 years and paper files until the pupil is aged 25. We hold Statement/EHCP documents until the pupil is aged 30.

5.4. Security

The Trust will take reasonable steps to ensure that members of staff will only have access to personal data relating to students and their parents where it is necessary for them to do so. All staff will be made aware of this policy and their duties under GDPR. The Trust and its organisations will ensure that all personal information is held securely and is not accessible to unauthorised persons. The Trust undertakes to ensure security of personal data by the following methods:

5.4.1 Physical Security

Appropriate building security measures are in place, such as alarms, deadlocks and computer hardware cable locks. Only authorised persons are allowed in the required areas. Disks, data sticks and printouts are stored securely when not in use. Visitors to the school and college are required to sign in and out, to wear identification badges whilst in the school or college and are, where appropriate, accompanied.

5.4.2 Computer Security

Security software is installed on all computers containing personal data. Only authorised users are allowed access to the computer files, and password changes are regularly undertaken. Computer files are backed up (i.e. security copies are taken) regularly.

5.4.3 Procedural Security

In order to be given authorised access to certain data, appropriate staff have to undergo checks and sign a confidentiality agreement within their contract. All staff are trained in their Data Protection obligations and their knowledge updated as necessary.

5.4.4 External Data Holders

Some data may be held externally to the Trust but, if so, the Trust will ensure that they process the data in a GDPR compliant manor. The trust will only share data with organisations that fall into the categories outlined on the privacy notice.

Overall security policy for data is determined by the Executive Principal and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. Any queries or concerns about security of data in the Trust's organisations should in the first instance be referred to the Executive Principal.

5.5 Data Controller and Data Protection Officer

Wootton Academy Trust is the Data Controller. It determines the purposes and means of processing data in line with the General Data Protection Regulation. The trust will also appoint a Data Protection Officer as it is a public body. The DPO will assist the trust in monitoring internal compliance, inform and advise on our data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

6. The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The rights that relate to our data subjects have been included in our Privacy Notice that is given out to the data subjects.

7. Rights of Access

The GDPR extends to all data subjects the right of access to their own personal data. Where a request for subject access is received from a student, the Trust's policy is that:

- Requests from students will be processed as a subject access request as outlined below and a copy of the information will be given directly to the student, unless it is clear that the student does not understand the nature of the request.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents.

- Requests from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent.

7.1. Processing Subject Access Requests

Requests for access must be made in writing to the Data Controller, and responses will be made as soon as is practicably possible and in accordance with legally-prescribed timescales. This is no more than a month from the date of the request however the trust will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary. Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of the request will be deemed to be the date on which sufficient information has been provided. The contact details are provided on the Privacy Notices.

The Trust may take legal advice in determining what information may be released. Certain data is exempt from the right of access under the GDPR, and this may include:

- Information that identifies other individuals,
- Information that the School or College reasonably believes is likely to cause damage or distress,
- Information that is subject to legal professional privilege,
- Student test scripts.

Unless otherwise stated, the Trust's organisations will treat as confidential any reference they give.

The Trust acknowledges that an individual may have the right to access a reference relating to them which is received by the Academy. Such references will only be disclosed if such disclosure does not identify the source of the reference, or if the referee has given their consent, or if disclosure is reasonable in the particular circumstances.

7.2. Exemptions

Certain data is exempted from the provisions of the GDPR. Information relating to the following will not be released to individuals:

- The prevention or detection of crime;
- The assessment of any tax or duty;
- Where the processing is necessary to exercise a right or obligation conferred or imposed by law upon the Trust.

The above are examples only of some of the exemptions under the Regulation. Parents and students should note that any information relating to child protection, or which reveals the identity of another student, will not be released.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, the Trust can:

- charge a reasonable fee taking into account the administrative costs of providing the information; or
- refuse to respond.

Where the trust refuses to respond to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

8. Disclosure of Information

A **legal disclosure** is the release of personal information to someone who requires the information to do his or her job within, or for, the school or college, provided that the purpose of that information has been registered.

An **illegal disclosure** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Trust's organisations registered purposes.

The Trust will, in general, only disclose data about individuals with their consent. However, there are circumstances under which the Trust's organisations may disclose data without explicit consent for that occasion. The categories of recipients have been outlined on the privacy notice. These are lists below:

- schools that the pupils attend after leaving us
- our local authority
- the Department for Education (DfE)
- Health and Education professionals
- Communication providers
- Providers who support the tracking of pupil learning
- The multi-agency panel
- Payment and security systems

Data used within the Trust by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the school or college who needs to know the information in order to do their work. The Trust's organisations will not disclose anything on students' records which would be likely to cause harm to the physical or mental health of the individual or that of anyone else.
The Trust's organisations may receive requests from third parties to disclose personal data it holds about students or their parents. The Trust's organisations confirm that they will not generally disclose information unless the individual has given their consent, or where one of the specific exemptions under the GDPR applies. When one of the Trust's organisations receives a disclosure request from a third party, it will take all reasonable steps to verify the identity of that third party before making any disclosure.

The Trust maintains an information audit that documents the data that it collects and the organisations that data is shared with.

9. Use of Personal Information by the Trust's Organisations the require permission

The school or college will, from time to time, make use of personal data relating to students and their parents in the following ways that require permission. Permission will have to be explicitly given and will be collected when the pupil joins the trust. Should a parent wish to limit or object to any such use, please notify the Trust in writing. These are as follows:

- Provide information beyond name, address and date of birth to the youth support service.
- Pictures to be used in school displays, in our printed prospectus, newsletter, websites, social media platforms or included in an external media article.
- Information from the fingerprint of my child being taken and used by Wootton Academy Trust as part of an automated biometric recognition system for access to the school's library system, catering facilities and personal student printing.

10. Enforcement

Individual members of staff can be personally liable in law under the terms of The GDPR. They may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

If an individual believes that the Trust or one of its organisations has not complied with this policy or acted otherwise than in accordance with The GDPR, they should utilise the complaints procedure and should also notify the Executive Principal.

11. Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.
Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

11.1 Obligation for data processor to notify data controller

- The data processor will notify the data controller without undue delay after becoming aware of the breach.

11.2 Obligation for data controller to notify the supervisory authority

- The data controller will notify the supervisory authority under GDPR if it's likely to result in a risk to people's rights and freedoms. This decision should be taken in consultation with the Executive Principal and the Data Protection Officer.
- Notification to the ICO to be made without undue delay and not later than 72 hours.
- Description of the nature of the breach
  - Categories of data
  - Approximate numbers of records and data subjects affected
- Describe likely consequences
- Describe measures taken – or to be taken – to mitigate the breach
- Communicate details of the Data Protection Officer
- There is no requirement to notify if unlikely to result in a risk to the rights and freedoms of natural persons (Article 33, clause 1)
- If the trust fails to report within 72 hours this must be explained to the ICO
- The Trust must document personal data breaches, effects and remedial action. This will enable assessment of compliance with these requirements.

11.3 Obligation for data controller to communicate a personal data breach to data subjects

- The trust must communicate to the data subject without undue delay if a high risk. The decision to communicate should be taken in consultation with the Executive Principal and the Data Protection Officer.
- Communication will be in clear plain language
- The supervisory authority may compel communication with data subject
- Exemptions if:
  - appropriate technical and organisational measures taken
  - high risk to data subject will not materialise
  - communication with data subject would involve disproportionate effort