Statutory Policy	
Initial Policy:	Mar 2016
Updated:	Nov 2020
Next Review:	Nov 2021
Key Person:	MLL

WILDERN ACADEMY TRUST

Data Protection

Principles

Wildern Academy Trust is committed to protecting and respecting the confidentiality of sensitive information relating to staff, students, parents, Members, Trustees and Local Governors of the governing body. This policy is to ensure that personal information is dealt with properly and securely in accordance with The Data Protection Act 2018 (DPA) and referred to in the General Data Protection Regulation (GDPR) as personal data.

The Trust collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. This information is gathered in order to enable the provision of education and other associated functions. In addition, the school may be required by law to collect, use and share certain information.

The Trust is the Data Controller under the Act and the Trust Board are ultimately responsible for its implementation. However, the School will deal with day to day matters.

The Trust has a Data Protection Officer, M Knight, who may be contacted at dataprotection@wildern.org

The Trust issues Privacy Notices (also known as a Fair Processing Notices) to all pupils/parents and staff. These summarise the personal information held about pupils and staff, the purpose for which it is held and who it may be shared with. It also provides information about an individual's rights in respect of their personal data.

Data Protection Principles
The GDPR establishes six principles as well as a number of additional duties that must be adhered to at all times:

1. Personal data shall be processed lawfully, fairly and in a transparent manner

2. Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (subject to exceptions for specific archiving purposes)

3. Personal data shall be adequate, relevant and limited to what is necessary to the purposes for which they are processed and not excessive;

4. Personal data shall be accurate and where necessary, kept up to date;

5. Personal data shall be kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

6. Personal data shall be processed in a manner that ensures appropriate security of the personal

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.

There is stronger legal protection for more sensitive information, such as:

- Ethnic background.
- Political opinions.
- Religious beliefs.
- Health.
- Sexual health.
- Criminal records.

All staff who process or use personal data must ensure that they follow these principles at all times. This policy has been created to ensure that happens. This policy does not form part of the contract of employment for staff, but it is a condition of employment that employees will abide by these rules and policy.

Purpose
This policy sets out how the school deals with personal information correctly and securely and in accordance with the GDPR, and other related legislation.

This policy applies to all personal information however it is collected, used, recorded and stored by the school and whether it is held on paper or electronically.

What is Personal Information/ data?
Personal information or data means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified, directly or indirectly by reference to details such as a name, an identification number, location data, an online identifier or by their physical, physiological, genetic, mental, economic, cultural or social identity. Personal data includes (but is not limited to) an individual's, name, address, date of birth, photograph, bank details and other information that identifies them.

Duties
Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Controllers have a General Duty of accountability for personal data.

Commitment

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

- Inform individuals of the identity and contact details of the data controller
- Inform individuals of the contact details of the Data Protection Officer
- Inform individuals of the purposes that personal information is being collected and the basis for this
- Inform individuals when their information is shared, and why and with whom unless the GDPR provides a reason not to do this.
- If the school plans to transfer personal data outside the European Economic Area (EEA) the school will inform individuals and provide them with details of where they can obtain details of the safeguards for that information
- Inform individuals of their data subject rights
- Inform individuals that the individual may withdraw consent (where relevant) and that if consent is withdrawn that the school will cease processing their data although that will not affect the legality of data processed up until that point.
- Provide details of the length of time an individual's data will be kept
- Should the school decide to use an individual's personal data for a different reason to that for which it was originally collected the school shall inform the individual and where necessary seek consent
- Check the accuracy of the information it holds and review it at regular intervals.

- Ensure that only authorised personnel have access to the personal information whatever medium (paper or electronic) it is stored in.
- Ensure that clear and robust safeguards are in place to ensure personal information is kept securely and to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded.
- Ensure that personal information is not retained longer than it is needed.
- Ensure that when information is destroyed that it is done so appropriately and securely.
- Share personal information with others only when it is legally appropriate to do so.
- Comply with the duty to respond to requests for access to personal information (known as Subject Access Requests).
- Ensure that personal information is not transferred outside the EEA without the appropriate safeguards.
- Ensure that all staff, Members, Trustees and Local Governors are aware of and understand these policies and procedures.

Practice

The following strategies will be used as appropriate to meet the principles above; the School will:

- Tell you what purposes we will use information for when we collect it.
- If information is shared we will tell you why, with whom and under what circumstances.
- Check the quality and accuracy of the information we hold.
- Apply Hampshire County Council's (HCC) current version of the School Records Retention Schedule 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 to safeguard personal information whether it is held in paper files or on our computer system.
- Share personal information with others only 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 in the Data Protection Act.
- Train our staff so that they are aware of our policies and procedures.
- This policy will be updated as necessary to reflect best practice or amendments made to the Data Protection Act.

The Data Controller and Designated Data Controllers
The Trust has identified its designated controllers as the Executive Headteacher, Headteachers, the Director of Support Services and Business support staff.

Any member of staff, parent or other individual who considers that the policy has not been followed in response of personal data about himself or herself or their child should raise the matter with the Executive Headteacher in the first instance.

Responsibilities of Staff
All staff are responsible for:
- Checking that any information that they provide to the Trust in connection with their employment is accurate and up to date.
- Informing the Trust of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The Trust cannot be held responsible for any errors unless the staff member has informed the Trust of such changes.
- Handling all personal data (e.g. student attainment data) with reference to this policy.

Data Security
All staff are responsible for ensuring that:
- Any personal data that they hold is kept securely.
- Personal information is not disclosed either orally or in writing or via Web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should:

- Be kept in a lockable, filing cabinet, drawer, or safe in a secure office,
- If it is computerised, it should be encrypted and password protected both on a local hard drive and on a network drive that is regularly backed up. All devices, including phones, should be password protected on boot.
- Not be kept on removable storage media such as USB memory sticks.

Rights to Access Information

All staff, parents and other users are entitled to:

- Know what information the School holds and processes about them or their child and why.
- Know how to gain access to it.
- Know how to keep it up to date.
- Know what the School is doing to comply with its obligations under the 1998 Act.

The Trust will, upon request, provide all staff and parents and other relevant users with a statement regarding the personal data held about them. This will state all the types of data the School holds and processes about them, and the reasons for which they are processed.

All staff, parents and other users have a right under the 1998 Act to access certain personal data being kept about them or their child either on computer or in certain files. Any person who wishes to exercise this right should make a request in writing and submit it to the Executive Headteacher. The School will ask to see evidence of your identity, such as your passport or driving license, before disclosure of information.

The Trust may make a charge on each occasion that access is requested in order to meet the costs of providing the details of the information held.

The Trust aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within the statutory period, as required by the 1998 Act. Any delay will be explained in writing to the person making the request. Access to non-personal data will be dealt with under the Freedom of Information Act 2000.

Exemptions

Wildern Academy Trust must not communicate anything to the parent which it could not communicate to the student him/herself under the DPA.

CCTV

CCTV within each school will only be used in public areas, which include toilet hand wash areas but they will not intrude on anyone's privacy. They will also be used for security purposes. Notices are placed in school to ensure that all visitors and staff are aware of this. Further information is available in the schools CCTV policy.

Photographs and Video

Refer to the School Photograph policy.

Third Parties

We are required, by law, to pass certain information about our students to our local authority (LA) and the Department for Education (DfE).

Wildern Academy Trust will ensure that any service providers used that will handle personal data comply with the DPA. We will not give information to third parties without consent unless the law and our policies allows us to.

For more information about how our local authority and DfE collect and use data please visit https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Retention of Data
Wildern Acadamy Trust has a duty to retain some staff and student personal data for a period of time following their departure from the schools, mainly for legal reasons, but also for other purposes such as being able to provide references. Different categories of data will be retained for different periods of time.

We keep all student records until they are 25 and staff records for 7 years. Records are either archived or kept on the system.

Destruction and Archive of Data
Records are kept in secure archive. Paper records are then shredded via a confidential shredding service, in line with DPA requirements.

Electronic systems are password encrypted.

All electronic devices are wiped of data before disposal.

Sensitive Personal Data
Wildern Academy Trust may, from time to time, be required to process sensitive personal data regarding an employee or a student, their parents or guardians. Sensitive personal data includes medical information and data relating to religion, race or criminal records and proceedings, including biometric information. Where sensitive personal data are processed by the Trust, the explicit consent of the appropriate individual will generally be required in writing.

Complaints
Complaints under this policy should be made to the Chair of the Trust Board who will decide if it is appropriate for the complaint to be dealt with under the complaints procedure. Complaints which are not dealt with under the Trust's complaints procedure should be forwarded in writing to the Information Commissioner (ICO). It is likely that complaints about procedural issues, due process and timeliness will be dealt with by the Trust Board; complaints that involve consideration of personal data or sensitive personal data should be referred to the Information Commissioner who can be contacted at Wycliffe House, Water Lane Wilmslow Cheshire SK9 5AF or at www.ico.gov.uk

Linked Policies:
Attendance Policy
Child Protection Policy
Code of Conduct for staff
Complaints Policy
CCTV Policy
Equality Policy
E-Safety Policy
Health and Safety at Work Policy
Information, Communication Technology (ICT) Policy
Protected Disclosures (Whistleblowing) Policy
Protection of Biometric Information
Publication Schemes (FOI) Policy
Safeguarding Policy
School Photograph Policy
Staff Discipline, Conduct and Grievance Policy
Supporting Students at school with medical conditions Policy
Wildern Assessment Data (WAD) Policy