Windsor Academy Trust

Policy: Data Protection Policy	
Responsible Committee:	People and Culture Committee
Date approved by the Board of Directors:	13th July 2023
Implementation date:	September 2023
Next review date:	September 2024

1. Introduction

1.1 This policy outlines Windsor Academy Trust's (WAT's) obligations under the data protection legislation. Whilst the European Union's (EU) General Data Protection Regulation (GDPR) is an EU Regulation and no longer applies to the UK, the Data Protection Act 2018 (DPA 2018) continues to apply. The provisions of the EU GDPR were incorporated directly into UK law at the end of the transition period and UK GDPR sits alongside the DPA 2018 with some technical amendments so that it works in a UK only context. The Information Commissioner's Office (ICO) continues to remain the independent supervisory body regarding the UK's data protection legislation.

1.2 Data protection is about regulating the way that WAT uses and stores information about identifiable people (Personal Data). It also gives people various rights regarding their data such as the right to access the Personal Data that WAT holds about them. WAT collects, stores and processes Personal Data including information about its members, directors, staff, pupils/students, volunteers, parents/carers, suppliers and other third parties and recognises that the correct and lawful treatment of personal data is important in maintaining confidence in WAT and in how it operates.

1.3 WAT's Board of Directors is ultimately accountable for how personal information is handled and has overall responsibility for ensuring that the trust complies with all relevant data protection obligations. The Headteacher is the representative of the Chief Executive Officer (CEO) who is the data controller, on a day-to-day basis. In this policy, the term "WAT" means both the academy and the central team.

1.4 WAT has appointed Judicium Education, a company that specialises in data protection, as the trust Data Protection Officer. Judicium will support the Director of Operations (DoO) in the development and implementation of data protection policies. Each school within WAT has a Data Protection Lead who has direct contact with Judicium Education consultants as part of the trust agreement, Judicium will also monitor compliance with data protection law across the trust. Judicium contact details are on the WAT website.

1.5 The DPO reports to the Director of Operations (DoO) who reports to the highest level of management at the trust as required by the UK GDPR. Each individual academy will have a Data Protection Lead (DPL) who will lead on Data Protection issues locally and will be advised by, and work with, the DPO. The DPO is the first point of contact for individuals whose data the academy processes, and for contact with the ICO.

1.6 All queries concerning data protection matters should be raised with the academy DPL in the first instance who will liaise with the DPO as required.

2. Application

2.1 This policy is applicable to all people working in WAT (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities. Any breach of this policy may result in disciplinary action.

2.2 This policy does not form part of an employee's contract of employment and may be amended by WAT at any time.

3. Information that falls within the scope of this policy

3.1 The data protection law concerns information about individuals.

3.2 Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and

pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

3.3 Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

3.4 Examples of places where Personal Data might be found are:

- On a computer database.
- In a file, such as a pupil report.
- A register or contract of employment.
- Pupils/student's' exercise books, coursework and mark books.
- Health records.
- Email correspondence.

3.6 Examples of documents where Personal Data might be found are;

- a report about a child protection incident;
- a record about disciplinary action taken against a member of staff;
- photographs/images of pupils/students;
- a recording of a teacher assessment;
- contact details and other personal information held about pupils, parents and staff and their families;
- contact details of a member of the public who is enquiring about placing their child at the academy;
- financial records of a parent/carer;
- information on a pupil's/student's performance; and
- an opinion about a parent/carer or colleague in an email.

3.7 Categories of Critical Personal Data:

3.7.1 The following categories are referred to as **Critical Personal Data (Special Category Data).** Particular care must be taken when dealing with Critical Personal Data which falls into any of the categories below;

- information concerning child protection matters;
- information about serious or confidential medical conditions and information about special educational needs;
- information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- financial information (for example about parents and staff);
- information about an individual's racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition;
- sex life or sexual orientation;
- genetic information;
- information relating to actual or alleged criminal activity; and
- biometric information (e.g. a pupil's fingerprints).

4. WAT's Obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

What does this mean in practice?

4.1.1 Processing data is any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

4.1.2 Individuals must be told what data is collected about them, what it is used for, and who it might be shared with. They must also be given other information, such as, what rights they have in their information, how long it is kept for and about their right to complain to the Information Commissioner's Office (ICO), the data protection regulator (see para 1.1). This information is provided in the WAT's privacy notices and can be obtained from the WAT websites.

4.1.3 If Personal Data is being used in a way that does not comply with data protection law, this should be raised with the DPL or DPO.

4.2 Personal Data must only be processed for the following purposes:

- To ensure that WAT provides a safe and secure environment.
- To provide pastoral care.
- To provide education and learning for pupils/students.
- To provide additional activities for pupils/students and parents/carers (for example activity clubs).
- To protect and promote the WAT's interests and objectives (for example fundraising).
- To safeguard and promote the welfare of-pupils/students.
- To perform a task in the public interest or in order to carry out official functions as authorised by law

- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract

4.2.1 If there is a need to process Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), it would be appropriate to contact the DPL/DPO to ensure that a lawful reason for using the Personal Data has been identified.

4.2.2 In some instances, consent may need to be obtained from the individual to use their Personal Data which must meet certain requirements. Further advice on obtaining consent can be sought from the DPL/DPO.

4.3 Personal Data must only be processed for limited purposes and in an appropriate way

What does this mean in practice?

4.3.1 Personal Data should only be used for the purposes that it has been collected. For example, if pupils/students are told that they will be photographed to enable staff to recognise them when writing references, the photographs should not be used for another purpose (e.g. in WAT's prospectus). Please see the WAT's Child Protection and Safeguarding and E-Safety Policies and guidance note relating to the use of images. The Code of Conduct also provides further information relating to the appropriate use of Personal Data.

4.4 Personal Data held must be adequate and relevant for the purpose

What does this mean in practice?

4.4.1 WAT will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data. [Please refer to the School's Data Retention Policy for further guidance].

4.5 Personal Data held must not be excessive or unnecessary

What does this mean in practice?

4.5.1 Personal Data must not be processed in a way that is excessive or unnecessary. For example, information should only be collected about a pupil's/student's medical history if that Personal Data has some relevance, such as allowing WAT to care for the pupil/student and meet their medical needs.

4.6 The Personal Data must be accurate

What does this mean in practice?

4.6.1 The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

4.7 Personal Data must not be kept for longer than necessary

What does this mean in practice?

4.7.1 WAT has an Information and Records Retention Policy which contains details about how long different types of data should be kept and when records should be destroyed. This applies to both paper and electronic documents. Care needs to be taken especially when deleting data.

4.7.2 The DPL/DPO should be contacted if further guidance on the retention periods and secure deletion is required.

4.8 Personal Data must be kept secure

What does this mean in practice?

4.8.1 All policies and guidance relating to the handling of Personal Data must be complied with, these include the policies outlined in section 4.3 and WAT's Information Security and Acceptable Use Policy.

4.9 Personal Data must not be transferred outside the UK without adequate protection

What does this mean in practice?

4.9.1 If personal data needs to be transferred outside the UK please contact the DPL/DPO. For example, if a school trip abroad is being arranged.

WAT and ist schools should not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

5. Sharing Personal Data

5.1 The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. The following points will be considered:

- Whether the third party has a need to know the information for the purposes of providing the contracted services;
- Whether sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- Whether the third party has agreed to comply with the required data security standards, policies and procedures and implemented adequate security measures;
- Whether the transfer complies with any applicable cross border transfer restrictions; and
- Whether a fully executed written contract that contains UK GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities for example, the Local Authority, 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 the School shall be clearly defined within written notifications including details and the basis for sharing the data.

5.1 Sharing Personal Data outside of WAT - dos and don'ts

5.1.1 **DO** share Personal Data on a "need to know" basis and think about why it is necessary to share data outside of the trust.

5.1.2 **DO** encrypt emails which contain Critical Personal Data/Special Category Data described in paragraph 3.7. For example, encryption should be used when sending details of a safeguarding incident to social services. The Information Security and Acceptable Use Policy provides more information.

5.1.3 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. Seek advice from the DPL/DPO if there is any suspicion as to why the information is being requested or if there are concerns about the identity of the requester (e.g. if a request has come from a parent/carer but using a different email address).

5.1.4 **DO** be aware of phishing. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

5.1.5 **DO NOT** disclose Personal Data to contractors without consulting the DPL/DPO. This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil/student recruitment event.

5.2 Sharing Personal Data within WAT

5.2.1 This section applies when Personal Data is shared within the academy or across the trust.

5.2.2 Personal Data must only be shared on a "need to know" basis.

5.2.3 The following are examples of sharing which are **likely** to comply with the data protection legislation:

- A teacher discussing a pupil's/student's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil/student).
- Informing an exam invigilator that a particular pupil/student suffers from panic attacks.
- Disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

5.2.4 The following are examples of sharing which are **unlikely** to comply with the data protection legislation;

- informing all staff that a pupil/student has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil/student); and
- Disclosing personal contact details for a member of staff (e.g. their home address and telephone number, birthday) to other members of staff (unless the member of staff has given permission or it is an emergency).

5.2.5 Personal Data may be shared to avoid harm, for example in child protection and safeguarding matters. WAT has a Child Protection and Safeguarding Policy which should be referred to and training must include the sharing of information relating to welfare and safeguarding issues.

5.3 Thinking about privacy on a day to day basis

5.3.1 WAT is required to carry out an assessment of the privacy implications of using Personal Data in certain ways such as when new technology is introduced, where the processing results in a risk to an individual's privacy or where Personal Data is used on a large scale.

5.3.2 These assessments referred to as Data Protection Impact Assessments are required to identify the measures needed to prevent information security breaches from taking place.

5.3.3 Where there is a need to share personal data with a third party, due diligence must be carried out and reasonable steps taken to ensure that all personal data is adequately protected. Further information can be found using the following link Contracts and data sharing | ICO

5.4 Individuals' rights in their Personal Data

5.4.1 People have various rights in their information. These rights can be exercised either in writing (e.g. in an email) or orally.

5.4.2 Please let the DPL/DPO know if anyone (either for themselves or on behalf of another person, such as their child);

- wants to know what information WAT holds about them or their child;
- asks to withdraw any consent that they have given to use their information or information about their child;
- wants WAT to delete any information;

- asks WAT to correct or change information (unless this is a routine updating of information such as contact details);
- asks for electronic information which they provided to WAT to be transferred back to them or to another organisation;
- wants WAT to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the Trust Newsletter or alumni events information; or
- objects to how WAT is using their information or wants WAT to stop using their information in a particular way. For example, if they are not happy that information has been shared with a third party.

5.5 Requests for Personal Data (Subject Access Requests)

5.5.1 One of the most commonly exercised rights is the right to make a Subject Access Request (SAR). Under this right people are entitled to request a copy of the Personal Data which WAT holds about them (or in some cases their child) and to certain supplemental information. Receiving a SAR involves complex legal rights. Staff must never respond to a SAR themselves without consulting the DPL/DPO.

5.5.2 SARs do not have to be labelled as such and do not even have to mention data protection. For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid SAR. The DPL must be informed if a request is received as outlined in the flowchart at Appendix A who will contact the DPO for advice on the response.

5.5.3 Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a SAR with respect to their child, the child must either be unable to understand their rights and the implications of a SAR, or have given their consent. Children's rights under the GDPR is explained in more detail.

5.5.4 Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at primary academies may be granted without the express permission of the pupil. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

5.5.5 Children aged ~~13~~ 12 and above are generally regarded to be mature enough to understand their rights and the implications of a SAR. Therefore, most SARs from parents or carers of pupils at an academy may not be granted without the express permission of the pupil/student. This is not a rule and an individual's ability to understand their rights will always be judged on a case-by-case basis.

5.5.6 When a SAR is made, WAT is required to disclose all of that person's Personal Data which falls within the scope of their request - there are only very limited exceptions and some examples are outlined at section 8.10.

5.5.7 The SAR must be acted upon without undue delay and at the latest within one month of receipt.

5.5.8 A month starts on the day the organisation receives the request, even if that day is a weekend or public holiday. The time limit should be calculated from the day the request is received (whether the day after is a working day or not) until the corresponding calendar date in the next month.

For Example

- WAT receives a request on 3 September. The time limit will start from the same day. This gives the trust until 3 October to comply with the request.
- If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month.
- If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.
- This means that the exact number of days to comply with a request varies, depending on the month in which the request was made.

5.5.9 A flowchart outlining the procedure to be followed on receipt of a SAR is attached at Appendix A and a log for recording and monitoring progress of the request is held by the DPL and WAT.

5.5.10 However, information should not be disclosed if it;

- might cause serious harm to the physical or mental health of the pupil/student or another individual;
- would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests;
- would include another person's personal data that cannot reasonably be anonymised, the other person has not provided consent and it would be unreasonable to proceed without it;.
- is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts;
- is a request that is unfounded or excessive, WAT may refuse to act on it, or charge a reasonable fee to cover administrative costs. WAT will take into account whether the request is repetitive in nature when making this decision; and
- when a request is refused, the individual will be told why, and informed that they have the right to complain to the ICO.

6. Biometric Recognition systems

6.1 Where biometric data is used within the trust as part of an automated biometric recognition system (for example, pupils use fingerprints to receive school dinners instead of paying with cash), WAT will comply with the requirements of the Protection of Freedoms Act 2012 and written consent will be obtained before any biometric data is taken and first processed.

6.2 Parents/carers will be notified before any additional biometric recognition system is put in place or before their child first takes part in it. The academy will get written consent from at least one parent/ carer before any biometric data is taken from their child and first processed.

6.3 Parents/carers and pupils have the right to choose not to use the academy's biometric system. Alternative means of accessing the relevant system will be provided for those pupils/students. Parents/carers and pupil/students can object to participation in the biometric recognition system(s), or withdraw consent, at any time;and any relevant data already captured will be deleted.

6.4 As required by law, if a pupil/student refuses to participate in, or continue to participate in, the processing of their biometric data; we will not process that data irrespective of any consent given by the pupil's/students and/or parent/carer.

6.5 Where staff members or other adults use the biometric system(s), consent will be obtained before they first take part in it, and alternative means of accessing the relevant service will be provided if they object. Staff and other adults can also withdraw consent at any time, and any relevant data already captured will be deleted.

7. CCTV and Body/Headcams

7.1 Where and whenever CCTV is used around any WAT locations to ensure the safety and security of sites, WAT will adhere to the CCTV Policy for the use of these cameras.

7.2 WAT does not need to ask individuals' permission to use CCTV, but will make it clear where individuals are being recorded. Any security cameras will always be clearly visible and there will be prominent signs explaining that CCTV is in use.

8. Photographs and Videos

8.1 As part of Trust activities, photographs are taken and images recorded of individuals WAT will obtain written consent for photographs and videos to be taken and used for communication, marketing and promotional materials. When using photographs and videos in this way they will not be accompanied with any other personal information about the child, to ensure they cannot be identified.

8.2 Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation.

9. Training

9.1 Directors, LAB members and staff will be provided with data protection training as part of their induction process.

9.2 Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

10 Personal data breaches

10.1 The Trust will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in the Data Breach Policy and Procedure.

11 Monitoring arrangements

11.1 The DPO is responsible for monitoring and reviewing this policy and his policy will be reviewed annually to reflect the Department for Education's recommendation in its advice on statutory policies.

Appendix A

Managing a Subject Access Request