Windsor Academy Trust

Policy: Data Protection Policy (for Staff)	
Responsible Committee:	Windsor Academy Trust, Board of Directors
Date revised by the Board of Directors:	11 July 2019
Implementation date:	1 September 2019
Next review date:	September 2021

1 Introduction

1.1 This policy is about your obligations under the data protection legislation. Data protection is about regulating the way that Windsor Academy Trust (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 on them.

1.2 WAT is ultimately responsible for how you handle personal information. In this policy, we use the term "WAT" to mean both the academy and the central team.

1.3 We will collect, store and process Personal Data about our trustees/ directors staff, pupils/students, volunteers, parents/carers, suppliers and other third parties. We recognise that the correct and lawful treatment of this data will maintain confidence in WAT and will ensure that WAT operates successfully.

1.4 You are obliged to comply with this policy when processing Personal Data on our behalf. Any breach of this policy may result in disciplinary action.

1.5 The Data Protection Officer (DPO) for WAT in the central team and the Data Protection Lead (DPL) in each academy are responsible for helping you to comply with WAT's obligations. All queries concerning data protection matters should be raised with your DPL in the first instance who will liaise with the DPO.

2 Application

2.1 This policy is aimed at all staff working in WAT (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, Local Advisory Board (LAB) Members, Directors, contractors, agency staff, work experience / placement, pupils/ students and volunteers.

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

3 What information falls within the scope of this policy

3.1 Data protection concerns information about individuals.

3.2 Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.

3.3 Information as simple as someone's name and address is their Personal Data.

3.4 In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

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

3.5.1 on a computer database;

3.5.2 in a file, such as a pupil report;

3.5.3 a register or contract of employment;

3.5.4 pupils' exercise books, coursework and mark books;

3.5.5 health records; and

3.5.6 email correspondence.

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

3.6.1 a report about a child protection incident;

3.6.2 a record about disciplinary action taken against a member of staff;

3.6.3 photographs/images of pupils/students;

3.6.4 a tape recording of a job interview;

3.6.5 contact details and other personal information held about pupils, parents and staff and their families;

3.6.6 contact details of a member of the public who is enquiring about placing their child at the academy;

3.6.7 financial records of a parent/carer;

3.6.8 information on a pupil's/student's performance; and

3.6.9 an opinion about a parent/carer or colleague in an email.

3.7 These are just examples - there may be many other things that you use and create that would be considered Personal Data.

3.8 **Categories of Critical Personal Data:** The following categories are referred to as **Critical Personal Data** in this policy and in the Information Security and Acceptable Use policy. You must be particularly careful when dealing with Critical Personal Data which falls into any of the categories below:

3.8.1 information concerning child protection matters;

3.8.2 information about serious or confidential medical conditions and information about special educational needs;

3.8.3 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);

3.8.4 financial information (for example about parents and staff);

3.8.5 information about an individual's racial or ethnic origin;

3.8.6 political opinions;

3.8.7 religious beliefs or other beliefs of a similar nature;

3.8.8 trade union membership;

3.8.9 physical or mental health or condition;

3.8.10 sex life or sexual orientation;

3.8.11 genetic information;

3.8.12 information relating to actual or alleged criminal activity; and

3.8.13 biometric information (e.g. a pupil's fingerprints following a criminal investigation).

4 Your obligations

4.1 Personal Data must be processed fairly, lawfully and transparently

4.1.1 What does this mean in practice?

(a) "Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data.

(b) Individuals must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (ICO, the data protection regulator).

This information is often provided in a document known as a privacy notice or a transparency notice. Copies of the WAT's privacy notices can be obtained from the ~~DPL or DPO~~ WAT websites. You must familiarise yourself with WAT's pupil/student, parent/carer and staff privacy notices.

(c) If you are using Personal Data in a way which you think an individual might think is unfair please speak to the DPL or DPO.

(d) You must only process Personal Data for the following purposes:

(i) ensuring that WAT provides a safe and secure environment;

(ii) providing pastoral care;

(iii) providing education and learning for our pupils/students;

(iv) providing additional activities for pupils/students and parents/carers (for example activity clubs);

(v) protecting and promoting the WAT's interests and objectives (for example fundraising);

(vi) safeguarding and promoting the welfare of our pupils/students; and

(vii) to fulfil WAT's contractual and other legal obligations.

(e) If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must contact the DPL/DPO. This is to make sure that WAT has a lawful reason for using the Personal Data.

(f) We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should contact the DPL/DPO if you think that you may need to obtain consent.

4.2 **You must only process Personal Data for limited purposes and in an appropriate way.**

4.2.1 What does this mean in practice?

(a) For example, if pupils/students are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in WAT's prospectus). Please see the Trust's Code of Conduct for further information relating to the use of photographs and videos and the Child Protection and Safeguarding E-Safety and Social Media Policies. A guidance note relating to the use of images can be obtained from the WAT website.

4.3 **Personal Data held must be adequate and relevant for the purpose**

4.3.1 What does this mean in practice?

(a) This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil/student.

4.4 **You must not hold excessive or unnecessary Personal Data**

4.4.1 What does this mean in practice?

(a) Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information 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.

4.5 **The Personal Data that you hold must be accurate**

4.5.1 What does this mean in practice?

(a) You must ensure that Personal Data is complete and kept up to date. For example, if a parent/carer notifies you that their contact details have changed, you should update WAT's information management system.

4.6 **You must not keep Personal Data longer than necessary**

4.6.1 What does this this mean in practice?

(a) WAT has an Information and Records Retention Policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data.

(b) Please contact the DPL/DPO if you require further guidance on the retention periods and secure deletion.

4.7 **You must keep Personal Data secure**

4.7.1 You must comply with the following policies and guidance relating to the handling of Personal Data:

(a) Information Security and Acceptable Use policy;

(b) Staff Code of Conduct:

(c) Information and Records Retention Policy; and

(d) Child Protection and Safeguarding Policy.

4.8 **You must not transfer Personal Data outside the EEA without adequate protection**

4.8.1 What does this mean in practice?

(a) If you need to transfer personal data outside the EEA please contact the DPL/DPO. For example, if you are arranging a school trip to a country outside the EEA.

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

5.1 Please review the following dos and don'ts:

5.1.1 **DO** share Personal Data on a need to know basis - think about why it is necessary to share data outside of the Trust - if in doubt - always ask The DPL/DPO.

5.1.2 **DO** encrypt emails which contain Critical Personal Data described in paragraph 3.8 above. For example, encryption should be used when sending details of a safeguarding incident to social services.

5.1.3 **DO** make sure that you have permission from the DPL/DPO to share Personal Data on the website.

5.1.4 **DO** be aware of "blagging". This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the DPL/DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent/carer but using a different email address).

5.1.5 **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.

5.1.6 **DO NOT** disclose Personal Data to the Police without permission from the DPL/DPO (unless it is an emergency).

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

6 Sharing Personal Data within WAT

6.1 This section applies when Personal Data is shared within WAT **OR** This section applies when Personal Data is shared between the academy and across WAT.

6.2 Personal Data must only be shared within WAT on a "need to know" basis.

6.3 Examples of sharing which are **likely** to comply with the data protection legislation:

6.3.1 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);

6.3.2 informing an exam invigilator that a particular pupil/student suffers from panic attacks; and

6.3.3 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).

6.4 Examples of sharing which are **unlikely** to comply with the data protection legislation:

6.4.1 informing all staff that a pupil/student has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil/student); and

6.4.2 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).

6.5 You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. WAT has a Child Protection and Safeguarding Policy which should be referred to. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please let your line manager know as a matter of urgency.

7 Individuals' rights in their Personal Data

7.1 People have various rights in their information.

7.2 You must be able to recognise when someone is exercising their rights so that you can refer the matter to the DPL/DPO. These rights can be exercised either in writing (e.g. in an email) or orally.

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

(i) wants to know what information WAT holds about them or their child;

(ii) asks to withdraw any consent that they have given to use their information or information about their child;

(iii) wants WAT to delete any information;

(iv) asks WAT to correct or change information (unless this is a routine updating of information such as contact details);

(v) asks for electronic information which they provided to WAT to be transferred back to them or to another organisation;

(vi) 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

(vii) 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.

8 Requests for Personal Data (Subject Access Requests)

8.1 One of the most commonly exercised rights mentioned in section 7 above is the right to make a subject access request. 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.

8.2 Subject access requests 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 subject access request. You must always immediately let the DPL/DPO know when you receive any such requests.

8.3 Receiving a Subject Access Request is a serious matter for WAT and involves complex legal rights. Staff must never respond to a Subject Access Request themselves unless authorised to do so.

8.4 When a subject access request is made, WAT must disclose all of that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

8.5 You must act on the Subject Access Request without undue delay and at the latest within one calendar month of receipt.

8.6 A calendar month starts on the day after the organisation receives the request, even if that day is a weekend or public holiday. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

8.7 ***For Example***

8.7.1 An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.

8.7.2 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.

8.7.3 If the corresponding date falls on a weekend or a public holiday, you have until the next working day to respond.

8.7.4 This means that the exact number of days you have to comply with a request varies, depending on the month in which the request was made.

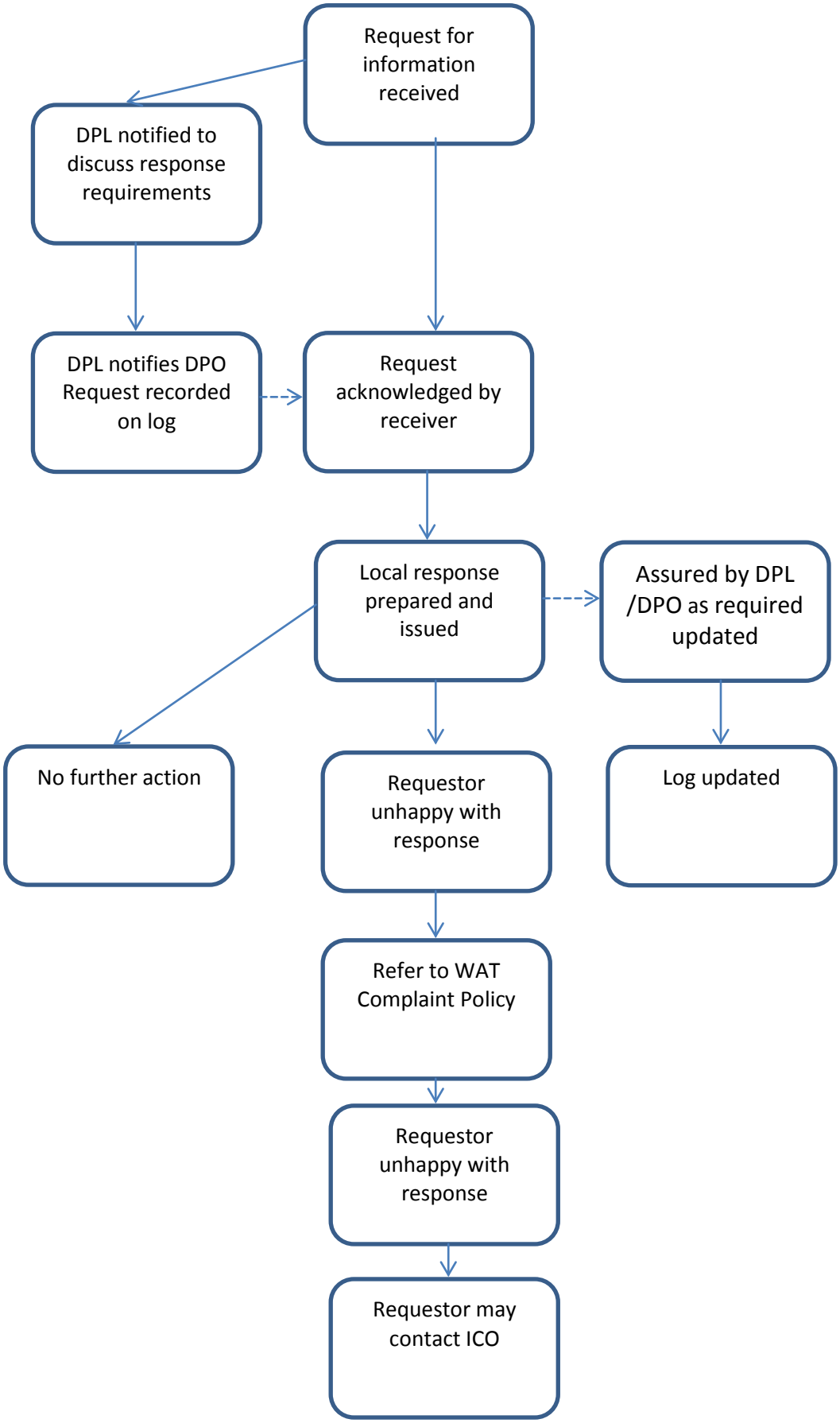
8.8 A flowchart outlining the procedure to be followed on receipt of a SAR is attached at Appendix A and a log for re cording and monitoring progress of the request is held at Appendix B.

9. Breach of this policy

9.1 Any breach of this policy may be treated as misconduct and could result in disciplinary action.

Appendix A

Managing a Subject Access Request



Appendix B

Windsor Academy Trust - Subject Access Requests Log

Our Ref	Date received	Date response due (one month)	Lead – response & action	Date Acknowledgement issued	Details of Enquirer	Details of request	Response & date