
# Windsor Academy Trust

| **Personal Data Handling Policy** | |
|---|---|
| **Responsible Committee:** | Windsor Academy Trust, Board of Directors |
| **Date revised by Board of Directors:** | December 2016 |
| **Next review date:** | December 2018 |

# Personal Data Handling Policy

## 1. Introduction

The trust and its employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the trust community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not;

- have permission to access that data, and/or
- need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the school into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office, for the trust and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (see WAT Data Protection Policy).

Due to the data sensitive nature of card processing activities, the Payment Card Industry Security Services Policy is also included as an appendix within the Personal Data Handling Policy.

This policy in its entirety to be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

## 2. Policy Statements

The trust will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”. (See Privacy Notice section below)

## 3. Personal Data

The school and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including/ students, members of staff and parents / carers e.g. names, addresses, contact details, legal guardianship contact details, health records, disciplinary records
- Curricular / academic data e.g. class lists, pupil / student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members.

## 4. Responsibilities

The school's Senior Information Risk Officer (SIRO) in each academy will keep up to date with current legislation and guidance and will:

- determine and take responsibility for the school's information risk policy and risk assessment
- appoint the Information Asset Owners (IAOs); (may also be the SIRO)

The academy will identify Information Asset Owners (IAOs) for the various types of data being held (e.g. pupil / student information / staff information / assessment data etc.). The IAOs will manage and address risks to the information and will understand:

- what information is held, for how long and for what purpose,
- how information has been amended or added to over time, and
- who has access to protected data and why.

Everyone in the academy has the responsibility of handling protected or sensitive data in a safe and secure manner.

Directors and Lab members across the trust are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role.

## 5. Registration

The WAT is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

## 6. Information to Parents / Carers – the "Privacy Notice"

In order to comply with the fair processing requirements of the DPA, the academy will inform parents / carers of all pupils / students of the data they collect, process and hold on the pupils / students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers (through their Prospectus, newsletters, reports or a specific letter / communication, web site). Parents / carers of young people who are new to the school will be provided with the privacy notice (as above).

## 7. Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff
- Staff meetings / briefings / Inset
- Day to day support and guidance from Information Asset Owners

## 8. Risk Assessments

Information risk assessments will be carried out by Information Asset Owners to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

- Recognising the risks that are present;
- Judging the level of the risks (both the likelihood and consequences); and
- Prioritising the risks.

Risk assessments are an ongoing process and should result in the completion of an Information Risk Actions Form (example below):

| Risk ID | Information Asset affected | Information Asset Owner | Protective Marking (Impact Level) | Likelihood | Overall risk level (low, medium, high) | Action(s) to minimise risk |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

## 9. Impact Levels and protective marking

Following incidents involving loss of data, the Government recommends that the Protective Marking Scheme should be used to indicate the sensitivity of data. The Protective Marking Scheme is mapped to Impact Levels as follows:

| Government Protective Marking Scheme label | Impact Level (IL) | Applies to schools? |
|---|---|---|
| **Not Protectively Marked** | 0 | Will apply in schools |
| **Protect** | 1 or 2 | |
| **Restricted** | 3 | |
| **Confidential** | 4 | Will not apply in schools |
| **Highly Confidential** | 5 | |
| **Top Secret** | 6 | |

Most student / pupil or staff personal data that is used within educational institutions will come under the PROTECT classification. However some, e.g. the home address of a child (or vulnerable adult) at risk will be marked as RESTRICT.

The trust and its academies will ensure that all staff, independent contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher. Unmarked material is considered 'unclassified'. The term 'UNCLASSIFIED' or 'NON' or 'NOT PROTECTIVELY MARKED' may be used to indicate positively that a protective marking is not needed.

All documents (manual or digital) that contain protected or restricted data will be labelled clearly with the Impact Level shown in the header and the Release and Destruction classification in the footer.

Users must be aware that when data is aggregated the subsequent impact level may be higher than the individual impact levels of the original data. Combining more and more individual data elements together in a report or data view increases the impact of a breach. A breach that puts students / pupils at serious risk of harm will have a higher impact than a risk that puts them at low risk of harm. Long-term significant damage to anyone's reputation has a higher impact than damage that might cause short-term embarrassment.

Release and destruction markings should be shown in the footer e.g.. "Securely delete or shred this information when you have finished using it".

## 10. Secure Storage of and access to data

The trust will ensure that systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

- All users will use strong passwords which must be changed regularly. User passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on school equipment (this includes computers and portable storage media (where allowed). Private equipment (i.e. owned by the users) must not be used for the storage of personal data.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected,
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete.

The trust and its academies has a clear policy and set of procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups, use of “Cloud Based Storage Systems” (for example dropbox, Microsoft 365, google apps and google docs) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The trust will ensure that it is satisfied with controls put in place by remote / cloud based data services providers to protect the data.

As a Data Controller, the school is responsible for the security of any data passed to a “third party”. Data Protection clauses will be included in all contracts where data is likely to be passed to a third party.

All paper based Protected and Restricted (or higher) material must be held in lockable storage, whether on or off site.

The trust recognises that under Section 7 of the DPA, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject. Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure and destruction of data (see WAT Data Protection Policy).

## 11. Secure transfer of data and access outside of the Trust HQ/Academy

The Trust recognises that personal data may be accessed by users outside the normal workplace, or transferred to the LA or other agencies. In these circumstances:

- Users may not remove or copy sensitive or restricted or protected personal data from the school or authorised premises without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location
- Users must take particular care that computers or removable devices which contain personal data must not be accessed by other users (e.g. family members) outside the normal workplace
- When restricted or protected personal data is required by an authorised user from outside the organisation's premises (for example, by a member of staff to work from their home), they should preferably have secure remote access to the management information system or learning platform;
- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the organisation or authorised premises if the storage media, portable or mobile device is encrypted and is transported securely for storage in a secure location;
- Users must protect all portable and mobile devices, including media, used to store and transmit personal information using approved encryption software; and
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe, and advice should be taken from the local authority (if relevant) in this event.

## 12. Disposal of Data

The trust will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of personal data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance and other media must be shredded, incinerated or otherwise disintegrated for data.

*A Destruction Log should be kept of all data that is disposed of. The log should include the document ID, classification, date of destruction, method and authorisation.*

## 13. Audit Logging / Reporting / Incident Handling

It is good practice, as recommended in the "Data Handling Procedures in Government" document that the activities of data users, in respect of electronically held personal data, will be logged and these logs will be monitored by responsible individuals.

The audit logs will be kept to provide evidence of accidental or deliberate data security breaches – including loss of protected data or breaches of an acceptable use policy, for example.

The trust has a policy for reporting, managing and recovering from information risk incidents, which establishes:

- a "responsible person" for each incident;
- a communications plan, including escalation procedures;
- and results in a plan of action for rapid resolution; and
- a plan of action of non-recurrence and further awareness raising.

All significant data protection incidents must be reported through the SIRO to the Data Controller and to the Information Commissioner's Office.

## 14. Use of technologies and Protective Marking

The following provides a useful guide:

| | The information | The technology | Notes on Protect Markings (Impact Level) |
|---|---|---|---|
| **Academy life and events** | Academy terms, holidays, training days, the curriculum, extra-curricular activities, events, displays of pupils work, lunchtime menus, extended services, parent consultation events | Common practice is to use publically accessible technology such as academy websites or portal, emailed newsletters, subscription text services | Most of this information will fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |
| **Learning and achievement** | Individual pupil / student academic, social and behavioural achievements, progress with learning, learning behaviour, how parents can support their child's learning, assessments, attainment, attendance, individual and personalised curriculum and educational needs. | Typically academys will make information available by parents logging on to a system that provides them with appropriately secure access, such as a Learning Platform or portal, or by communication to a personal device or email account belonging to the parent. | Most of this information will fall into the PROTECT (Impact Level 2) category.<br>There may be students/ pupils whose personal data requires a RESTRICTED marking (Impact Level 3) or higher. For example, the home address of a child at risk. In this case, the trust/academy may decide not to make this pupil / student record available in this way. |
| **Messages and alerts** | Attendance, behavioural, achievement, sickness, school closure, transport | Email and text messaging are commonly used by schools to contact | Most of this information will fall into the PROTECT (Impact Level 1) |

| | | | |
|---|---|---|---|
| | arrangements, and other information that it may be important to inform or contact a parent about as soon as possible. This may be particularly important when it is necessary to contact a parent concerning information that may be considered too sensitive to make available using other online means. | and keep parents informed. Where parents are frequently accessing information online then systems e.g. Learning Platforms or portals, might be used to alert parents to issues via “dashboards” of information, or be used to provide further detail and context. | category. However, since it is not practical to encrypt email or text messages to parents, academys should not send detailed personally identifiable information. General, anonymous alerts about academy’s closures or transport arrangements would fall into the NOT PROTECTIVELY MARKED (Impact Level 0) category. |

**Appendix 1**:

## 1. Additional issues / documents related to Personal Data Handling in Schools:

### 1.1 Use of Biometric Information

The Protection of Freedoms Act 2012 includes measures that affect schools and colleges that use biometric recognition systems, such as fingerprint identification and facial scanning:

- For all pupils in schools and colleges under 18, they must obtain the written consent of a parent before they take and process their child's biometric data.
- They must treat the data with appropriate care and must comply with data protection principles as set out in the Data Protection Act 1998.
- They must provide alternative means for accessing services where a parent or pupil has refused consent.

The trust/academy will no longer be able to use pupils' biometric data without parental consent. The advice came into effect from September 2013. Schools may wish to consider these changes when reviewing their Personal Data Handling Template. Academies may wish to incorporate the parental permission procedures into existing parental forms (eg AUP / Digital & Video Images permission form).

### 1.2 Use of Cloud Services

The trust/academy should always carry out its due diligence and ensure that it has received full and comprehensive responses to the following questions:

- How often is the data backed up?
- Does the service provider have a clear process for you to recover data?
- Who owns the data that you store on the platform?
- How does the service provider protect your privacy?
- Who has access to the data?
- Is personal information shared with anyone else? Look out for opt in/opt out features
- Does the service provider share contact details with third party advertisers? Or serve users with ads?
- What steps does the service provider take to ensure that your information is secure?
- Is encryption used? Is https used as default or is there an option to use this? Two step verification?

- How will your data be protected? Look out for features that will keep your information safe and secure including Anti-spam, Anti-Virus and Anti-malware…
- How reliable is the system? Look out for availability guarantees.
- What level of support is offered as part of the service? Look out for online and telephone support, service guarantees

The academy should always liaise with the Strategic Lead for IT on the procurement of cloud based systems.

Parental permission for use of cloud hosted services: An academy using cloud hosting services (e.g. Google Aps for Education) may be required to seek parental permission to set up an account for pupils / students.

Google Apps for Education services - requires an academy to obtain 'verifiable parental consent'. Normally, it will incorporate this into their standard acceptable use consent forms sent to parents each year ("Parent / Carer Acceptable Use Agreement").

Privacy and Electronic Communications: The trust and its academies are subject to the Privacy and Electronic Communications Regulations in the operation of their websites.

**1.3 Freedom of Information Act**

All academies must have a Freedom of Information (FOI) Policy which sets out how it will deal with FOI requests. In this policy the academy should:

- Delegate to the Headteacher day-to-day responsibility for FOI policy and the provision of advice, guidance, publicity and interpretation of the academy's policy
- Consider designating an individual with responsibility for FOI, to provide a single point of reference, coordinate FOI and related policies and procedures, take a view on possibly sensitive areas and consider what information and training staff may need
- Consider arrangements for overseeing access to information and delegation to the appropriate governing body
- Ensure that a well-managed records management and information system exists in order to comply with requests
- Ensure a record of refusals and reasons for refusals is kept, allowing the trust to review its access policy on an annual basis

**1.4 Privacy Notice - Data Protection Act 1998 (refer to the WAT Data Protection Policy)**

Windsor Academy Trust is a data controller for the purposes of the Data Protection Act. The trust through its academies collects information from you and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

- Support your teaching and learning;
- Monitor and report on your progress;
- Provide appropriate pastoral care, and
- Assess how well your school is doing.

This information includes your contact details, assessment results, attendance information and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service and may also obtain from them details of any learning or qualifications you have undertaken.

Once you are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in your area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both your and your parent's/s' name(s) and address, and any further information relevant to the support services' role. However, if you are over 16, you (or your parent(s)) can ask that no information beyond names, address and your date of birth be passed to the support service.

Please inform your academy if you wish to opt-out of this arrangement. For more information about young peoples' services, please go to the Directgov Young People page at *www.direct.gov.uk/en/YoungPeople/index.htm*

***We will not give information about you to anyone outside the academy without your consent unless the law and our rules allow us to.***

We are required by law to pass some information about you to the Local Authority and the Department for Education (DfE)

We are also required by law to pass some information about you to the Department for Education (DfE) and, in turn, this will be available for the use(s) of the Local Authority.

If you want to see a copy of the information about you that we hold and/or share, please contact the academy.

If you require more information about how the Local Authority (LA) and/or DfE store and use your information, then please go to their respective websites:

### 1.5 PCI Compliance Policy

### Policy Statement

All card processing activities and related technologies must comply with the Payment Card Industry Data Security Standard (PCI-DSS) in its entirety. Card processing activities must be conducted as described herein and in accordance with the standards and procedures set out in this policy. No activity may be conducted nor any technology employed that might obstruct compliance with any portion of the PCI-DSS.

### Specific Policy Requirements

### Network Security

- All card payment terminals are mobile and not connected to the network, card data is also not stored electronically on the network.
- Firewalls are fully implemented to the network.
- Firewall and router configurations must restrict connections between untrusted networks.
- Firewalls must also be implemented to protect local network segments and the IT resources that attach to those segments such as the business network, and open network.
- No direct connections from Internet to cardholder data environment will be permitted. All traffic has to traverse through a firewall.

### Cardholder Data

- All sensitive cardholder data stored and handled by the trust and its employees must be securely protected against unauthorised use at all times. Any sensitive card data that is no longer required by the trust for business reasons must be discarded in a secure and irrecoverable manner.
- If there is no specific need to see the full PAN (Permanent Account Number), it has to be masked when displayed.

- Card holder data (PAN, track data etc.) must never be sent over the internet via email, instant chat or any other end user technologies.
- If there is a business justification to send cardholder data via email or via the internet or any other modes then it should be done after authorization and by using a strong encryption mechanism (i.e. – AES encryption, PGP encryption, IPSEC, GSM, GPRS, Wireless technologies etc.,).
- The transportation of media containing sensitive cardholder data to another location must be authorised by management, logged and inventoried before leaving the premises. Only secure courier services may be used for the transportation of such media. The status of the shipment should be monitored until it has been delivered to its new location.

**It is strictly prohibited to store:**

- The contents of the payment card magnetic stripe (track data) on any media whatsoever.
- The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever.
- The PIN or the encrypted PIN Block under any circumstance.

**Disposal of Stored Data**

- All data must be securely disposed of when no longer required, regardless of the media or application type on which it is stored.
- All hard copies of cardholder data must be manually destroyed when no longer required for valid and justified business reasons. A termly process must be in place to confirm that all non-electronic cardholder data has been appropriately disposed of in a timely manner.
- All cardholder information awaiting destruction must be held in lockable storage containers clearly marked “Confidential Waste” - access to these containers is restricted. The destruction of all hardcopy materials are crosscut shredded, incinerated or pulped so they cannot be reconstructed.
- The destruction of electronic data will require that it be unrecoverable when deleted.

**Maintenance of Vulnerability Management Program**

- All machines must be configured to run the latest anti-virus software as approved by the trust. The antivirus should have periodic scanning enabled for all the systems.
- The antivirus software in use will be capable of detecting all known types of malicious software (Viruses, Trojans, adware, spyware, worms and rootkits)
- All removable media (for example floppy and others) should be scanned for viruses before being used.
- Master Installations of the Antivirus software should be setup for automatic updates and periodic scans.
- End users must not be able to remove or adversely change the settings or alter the antivirus software.
- E-mail with attachments coming from suspicious or unknown sources should not be opened. All such e-mails and their attachments should be deleted from the mail system as well as from the trash bin. No one should forward any e-mail, which they suspect may contain virus.

**Access Control Measures**

- POS devices surfaces should be periodically inspected to detect tampering or substitution.
- Personnel using the devices receive training and are restricted to only those necessary for business purposes.
- Any 3rd party maintenance, updates or device replacement is arranged centrally by the finance manager only and the validity of any work is verified prior to work being carried out.
- Terminals are kept locked in either a secure room or safe outside of business hours, during business hours all terminals are in the constant presence of an employee and not left unattended.
- All receipts are kept securely during day-to day operations and then transferred to the finance office for secure storage.