**WESTFIELD ACADEMY DATA PROTECTION POLICY**

## 1. INTRODUCTION

This Data Protection Policy has been reviewed and re-written to incorporate the provisions of the General Data Protection Regulations (GDPR) and the Data Protection Act 2017.

This policy covers all personal data held by the Academy as the Data Controller. The Academy holds the personal data of Students, Parents and Staff. Personal Data is defined by the GDPR as:

*Any information relating to an identified or identifiable natural person, where an identifiable natural person is one who can be identified directly or indirectly, in particular by name, identification number, location data, online identifier or one or more factors specific the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person*

The Academy will abide by the provisions of the GDPR and the Data Protection Act 2017 and will seek to control the personal data it holds in a lawful, fair and transparent manner. The Academy will take all reasonable steps to ensure that partner organisations who process data on its behalf also abide by the provisions of GDPR and the Data Protection Act 2017.

Whilst the Academy's Governing Body may delegate management and implementation of Data Protection to the Principal and Data Protection Officer, it remains the responsibility of the Governing Body to ensure compliance with GDPR and the Data Protection Act.

## 2. DATA PROTECTION OFFICER

The Academy will appoint a Data Protection Officer (DPO) who will be responsible for the implementation of this policy and the overall management of data within the Academy. The DPO will be independent and will have sufficient authority to be able to implement changes to Academy working practices. The name of DPO will be shared with the Information Commissioner's Office and will be published on the school website and on all relevant paperwork including Privacy Notices.

The Academy will also identify a named Data Protection Governor who will be responsible for monitoring implementation of this policy.

## 3. FAIR, LAWFUL AND TRANSPARENT PROCESSING

The Academy controls the personal data of Students, Parents and Staff because it is necessary to do so in the public interest. The Academy may use this data without the consent of the individual providing it is for activities that it may reasonably be expected that the Academy will perform.

Where the Academy wishes to use the personal data for activities outside what may be reasonably expected then the clear and unambiguous consent of the individual must be obtained. Records of such consent must be kept.

The Data Protection Act 2017 states that a data subject over the age of 13 is responsible for giving consent to share their personal data. Therefore where the Academy requires consent to share the personal data of a student, this will be sought from parents when the student is below the age of 13, and from the student when aged 13 or over. Where there is a safeguarding concern parents may still be able to prevent data sharing when the student is over 13.

At times the Academy may need to use data to fulfil a legal obligation, in particular to protect the best interests of a student, meet its employment obligations or to respond in an emergency situation. In these circumstances consent is not required.

The Academy will produce a Privacy Notice for each of the groups that we hold personal data - Students, Parents and Staff. The Privacy Notices will be published on the academy's website and will clearly identify the type of data that is being held, the purpose that data is being used for and with whom the data is being shared. Students, Parents and Staff will be reminded at least annually of the existence of the Privacy Notice.

## 4. DATA SHARING

The efficient operation of the Academy requires that personal data is shared with a range of organisations, which will be identified on the Privacy Notice. The Academy may share this data providing it is for activities in the public interest.

The Academy, as the Data Controller, has a legal obligation to ensure that organisations with whom it shares data also comply by the GDPR and the Data Protection Act 2017. External organisations who are processing the Academy's data will be required to provide formal reassurance which confirms their compliance with these regulations.

## 5. DATA ACCURACY AND DESTRUCTION

The Academy will take all reasonable steps to ensure that the data it holds is accurate. Students, Parents and Staff will be asked annually to confirm the accuracy of the data that is held. In addition they will be reminded on the website and through newsletters and briefings to keep the Academy informed of changes to personal circumstances.

Where it becomes known that personal data is inaccurate, this will be deleted immediately and all reasonable efforts made to obtain the correct data.

The Academy will ensure that it reviews the data that it holds and will not keep that data longer than is required. In considering when data it holds should be destroyed the Academy will be guided by the timescales identified by the Institute of Records Management Toolkit for Schools. The Academy will ensure that destruction of data is carried out by a licensed contractor and that appropriate records of the destruction are maintained.

## 6. DATA SECURITY

### 6.1 Electronic storage of data

Personal data controlled by the Academy is stored electronically on local servers and may be shared with software providers and stored on the cloud. The Academy will maintain robust security systems to ensure the safety of this data and prevent unauthorised access or sharing.

Data Security is maintained by all users requiring to reset their Windows & G-Suite login credentials on a 3 monthly basis. Internet traffic that reaches the schools internal network is siphoned through our robust firewall which is hosted by a recognised and security accredited third party provider. Only recognised internet protocols will be allowed to reach the end user. All changes made to the firewall are logged and can be easily reverted.

Staff are required to lock their computer when leaving their desk and to be mindful of others in the room - especially students. Staff computers, when logged in but not in use, are set to automatically lock out within 10 minutes of inactivity. Students are also denied log on access to staff PCs via group policy enforcement and therefore are unable to log in and use a staff computer at school.

The Academy recognises that staff may wish to set up personal mobile devices to receive work emails or to access Google Documents whilst away from the school site. This information can also be accessed through a home based PC or chrome device.

Removing data from site increases the risk of a data breach and staff are required follow the procedures to reduce this risk. Staff who set up mobile devices to receive work emails or otherwise access personal data will:

1) Set up authentication on the device. This should be in the form of a PIN number, password, fingerprint or face recognition ID
2) Take all reasonable steps to protect the integrity of the authentication and ensure no other individual has set up access to that mobile device.
3) Where the authentication becomes known to others - take immediate steps to alter the authentication details.
4) Disable the email notifications which appear on the lock screen in the Settings menu.
5) Ensure auto screen lock is set to 1 minute or less.
6) Ensure the data on the mobile device is encrypted. For Apple IOS devices the encryption is automatic and no further steps are required. For Android devices encryption is an option under the Settings menu.
7) Avoid accessing personal data in a public place or when attached to an unsecured wi-fi network
8) Report to the Data Protection Officer any breach or suspected breach of personal data.

Staff who access personal data from a home based PC or other device will ensure:

1) A separate account is set up on the device which is protected by a password log in or other form of authentication.
2) Take all reasonable steps to protect the integrity of the authentication and ensure no other individual has set up access to that account.
3) That where the authentication becomes known to others - take immediate steps to alter the authentication details.
4) Login and logout of Google Chrome for each use.
5) They are aware of others in the room - and do not access or share personal data with others.
6) That personal data is not left on the screen and that they auto lock the device before walking away
7) They do not print personal data at home, unless there is an overwhelming reason to do so and the printed copies can be stored securely.

In a Google Chrome environment it is unnecessary to transfer data between home and school on a USB stick or other portable storage device. Therefore personal data will not be stored on a USB stick or other portable storage device.

If there are exceptional circumstances where no other data transfer solution is available, then the USB stick will be encrypted.

6.2 Paper based personal data

The Academy will ensure that paper based personal data will be securely stored. Such data will be locked away in secure filing cabinets and/or in storage rooms and offices that are lockable with restricted access to the keys.

Staff will not leave “sensitive” personal data visible on unmanned desks and will ensure this is stored securely.

Where possible staff should not remove personal data from the site, especially where this data contains sensitive information. Staff who remove personal data from the site assume full responsibility for its security and must take appropriate measures to ensure that this data is secure. Once the reason for removing the data from site is over then the data must be returned to the Academy for storage or destruction.

## 7. RIGHT TO ERASURE

Any data subject has the right to request that data held by the Academy is erased. In considering a request for erasure of data the Academy will need to decide whether continuing to hold the data is necessary for the efficient, safe and legitimate operation of the Academy and whether it can continue to hold the data in the public interest, so that it can fulfil its statutory responsibilities. In particular if the data subject is no longer part of the Academy, the appropriate length of time that the data should be held will need to be considered with reference to the Institute of Records Management guidance.

The Academy should respond in writing to requests for erasure, confirming erasure or providing grounds to indicate why erasure is not possible. Records of requests and responses should be kept.

## 8. SUBJECT ACCESS REQUESTS

All Data Subjects have the right to view personal data held by the Academy through a Subject Access Request (SAR). Where possible the request should be made on the Subject Access Request Form (Appendix 1), but all written requests however received must be treated as an SAR. The Academy has 40 days to respond in full to an SAR. No charge will be made for a SAR.

Parents/carers may make a SAR in relation to their son/daughter at the school, however the consent of the child should also be obtained for release of their personal data, unless it is judged that the child is unable to make an informed decision.

The Data Protection Officer must verify the identity of the person making the SAR. This may include requesting to see photo ID such as a passport or driving licence.

Once received the Data Protection Officer should acknowledge the SAR within 48 hours and where necessary seek clarification on the nature of the data requested. All staff within the Academy must co-operate with the DPO to assist in the collation of the requested data, ensuring all relevant data for the SAR is provided on time.

The DPO must ensure that the personal data of others is redacted from data provided through a SAR, and must take all reasonable steps to ensure the data provided is complete.

Where subject access requests are manifestly unfounded or excessive, in particular because they are repetitive, the Academy may:

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

Where the Academy refuses to respond to a request, an explanation will be provided to the individual, including their right to complain to the Information Commissioner's Office.

Records of all SARs should be kept.

## 9. DATA PROTECTION IMPACT ASSESSMENTS

Data Protection Impact Assessments (DPIAs) will help the Academy to identify the most effective way to comply with its data protection obligations and to meet individuals' expectations of privacy.

The Academy will carry out a DPIA when considering:

- using new technologies; and

- the processing is likely to result in a high risk to the rights and freedoms of individuals.

The Academy will follow guidance provided by the Information Commissioner's Office.

## 10. DATA BREACHES

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

When a data breach occurs the DPO must be informed immediately with as much information as possible. It will be the responsibility of the DPO to investigate the breach. The investigation should consider the cause of the breach, who has been affected, the seriousness of the breach and the actions that are required to prevent it happening again. A record of the investigation must be kept.

Where the data breach is likely to result in a risk to the rights and freedoms of individuals this must be reported to the Information Commissioner's Office within 72 hours. Where there is a high risk of to the rights and freedoms of individuals then the individuals themselves must be informed of the breach.

All data breaches that have been reported to the ICO should also be reported to the Governing Body via the Data Protection Governor. The Governing Body must ensure that robust and appropriate remedial action will be taken to prevent further similar data breaches.

Where a data breach has occurred through the actions of an individual failing deliberately or otherwise to implement the data protection policies of the Academy, this may lead to disciplinary action under the Academy's disciplinary policy.

## 11. STAFF TRAINING

The Academy recognises that the most likely breach of data security comes through human error. The likelihood of human error will be reduced where staff are fully aware of the correct procedures surrounding data protection and have regular reminders regarding their own role. All staff will be made aware of the contents of this policy and will receive training as part of the Academy's CPD programme and through induction. In addition the Academy will provide regular updates and reminders through staff meetings, and verbal or electronic briefings.

The Academy will ensure that the Data Protection Officer is appropriately trained and has a good understanding of the requirements of GDPR such that they may carry out their role effectively. Training will also be provided for the monitoring Governor.