Westfield Academy

Seeing the qualities in every child

Data Protection Policy

Approval Date – March 2017 Review Date – March 2019

Westfield Academy collects and uses personal information about staff, students, parents or carers and other individuals who come into contact with the school. This information is gathered in order to enable it to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. The Assistant Principal (Business) is the named Data Controller. Schools also have a duty to issue a Fair Processing Notice (Privacy Notice) to all students/parents or carers, this summarises the information held on students, why it is held and the other parties to whom it may be passed on. Information is also held on other users of school facilities.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

What is Personal Information?

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. (Applies to Students / Parents / Carers / Staff / Others)

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1) Personal data shall be processed fairly and lawfully;
2) Personal data shall be obtained only for one or more specified and lawful purposes;
3) Personal data shall be adequate, relevant and not excessive;
4) Personal data shall be accurate and where necessary, kept up to date;
5) Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6) Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7) Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8) 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.

Policy Statement
Westfield Academy is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures

Privacy Notice
In order to comply with the fair processing requirements of the DPA, the school will provide parents / carers of all students with a privacy notice. (Appendix 1.) This will summarise the data we collect, process and hold on students, the purposes for which the data is held and the third parties to whom it may be passed. Parents are asked to sign to acknowledge they have read and understood.

Complaints
Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Related Policies / Documents
E-Safety / ICT Acceptable Use Policy
Data Protection and E Safety Guidance for Staff (Appendix 2)

Review
This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years. The policy review will be undertaken by the Principal, or nominated representative.

Contacts
If you have any enquires in relation to this policy, please contact the Assistant Principal (Business) who will also act as the contact point for any subject access requests.
Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745

APPENDIX 1 PRIVACY NOTICE – DATA PROTECTION ACT 1998

We, Westfield Academy are the Data Controller for the purposes of the Data Protection Act. We are registered with the ICO (Information Commisioners Office). We collect information on pupils and parents and/or carers, and may receive information about pupils and parents and/or carers from previous schools. 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, national curriculum assessment results, attendance information, characteristics such as ethnic group, special educational needs and any relevant medical information.

We will not give information about you to anyone outside the school without your consent unless the law and our rules permit it.

We are required by law to pass some of your information to the Local Authority (LA), and the Department for Education (DFE).

We use a third party company, Groupcall Limited, for our first day of absence automated call system and for other messages to parents. The service they provide is the transmission of a text message, which contains only the child's first name and no other information, to the selected telephone numbers. They do not hold any personal data relating to parents/carers or pupils. Parents have the right to choose not to be included in the first day of absence Call System. (Please contact the attendance officer at the school if you wish to not be included).

We use a secure off- site backup service provided by Schoolcare which backs up encrypted versions of our data for emergency recovery.

We share some basic ID data on a temporary basis with the provider of our Parent Evening Booking service, School Cloud Systems.

We also share data from time to time with Career's South West (Student Career Advice), Inspire To Achieve (Student Support) and our Work Experience Partners.

If you wish to see a copy of the information we hold and share about you then please contact; Lisa Jeffreys, Principal's PA, at the school.

If you require more information about how the Local Authority (LA) and/or DfE store data please contact these institutions directly at the following addresses:

Public Communications Unit
Department for Education
Sanctuary Buildings
Great Smith Street
London
SW1P 3BT
Website: www.education.gov.uk
Email: info@education.gsi.gov.uk
Telephone: 0370 000 2288

Information Governance Officer
Somerset County Council
County Hall
Taunton
Somerset
TA1 4DY

Email: informationgovernance@somerset.gov.uk

Appendix 2: Data protection and E-Safety Guidance for Staff

Rationale

All staff must ensure that students are responsible and safe users of ICT. They should also ensure that they only use school technologies to support them in carrying out their professional role appropriately.

In particular where data is accessible on mobile devices or on computers outside of the school premises staff must ensure that they have appropriate safeguards in place to protect personal data.

Staff must not run the risk of making themselves personally vulnerable by using technologies to communicate inappropriately with students.

All staff must:

- Adhere to ICT acceptable users' policy and in particular to its purpose and principles whether on site or off site.
- Use the school ICT network for carrying out their job appropriately.
- Supervise students using ICT appropriately to ensure this policy is implemented.
- Ensure that students are using the system responsibly and that this policy is being adhered to using monitoring software where appropriate.
- Not use the school network for private purposes during normal school hours, or for trading with other users of the network for private gain.
- Be aware that the school network is not private, and that network managers can and do look at data.
- Never use ICT to engage in activities that may be in violation of the law.
- Have an up to date awareness of e-safety matters and of the current school e-safety and Data Protection policy and practices
- Not have present or past students as "friends" on social networking sites (for these purposes, past is defined as within the past 5 years).
- Not have contact details of students on their own personal devices.
- Report any break of this code, suspected misuse or problem to the E-Safety Co-ordinator / IT Manager as appropriate
- Have a strong password and ensure other users do not have access to it.
- Ensure computers are always locked when not in use.
- Apply the same principles of Data Protection to Off Site working as On Site working
- Be aware of the latest legislation regarding the movement of Student Data off the school network. All data moved (eg by USB stick, transfer to hard disk, laptop, tablet, mobile phone etc) must be encrypted. This includes any data transferred from remote access to a local (home) computer.
- They do not post on social media any comments about the School, Staff or Students which may bring the school into disrepute

Off site and Mobile Working

With the development of cloud based computing and mobile technology staff increasingly have access to personal data off site. All staff must ensure

- All devices that are able to access personal data including work based emails and school management systems are protected by passwords, pin numbers or fingerprint sign in <u>every time</u> the device is used
- The mobile device's auto lock setting is enabled and will lock the device after no more than one minutes inactivity
- Home based PCs or Chromebooks are password protected and screens are locked when left.
- They are aware who else may be able to view the screen whilst working at the PC and ensure sensitive data is not seen or shared inappropriately
- Personal data is never printed out offsite

Staff should note the section on ICT from the Staff Code of Conduct (Staff Handbook):

"ICT – Staff must use ICT for carrying out their job appropriately. It must not be used for private purposes including social networking during normal school hours or for trading with other network users. Staff must ensure privacy and data protection by ensuring their log-on password is confidential and must lock their computer when not in use. Staff must not use personal devices during the school day, must not keep personal contact details of students, ex-students or parents on personal devices and must not have any of these groups as "friends" when using social networking media. Staff must take reasonable steps to protect their professional integrity."

Inappropriate use will be subject to the Staff Disciplinary code.

Staff Name:_____

Staff Signature:_____

Date:_____