DROYLSDEN
Academy

Data Protection Policy (General Data Protection Regulation – GDPR) Registration No: ZA468261

Review Cycle: Two Years
Next Review Date: May 2024
Person Responsible: Business Manager/Data Protection Officer
Approving Body: Headteacher

General Data Protection Regulation

Our Commitment:

Droylsden Academy is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).
https://ico.org.uk/for-organisations/guide-to-data-protection/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements.

The legal bases for processing data are as follows –

(a) Consent: the member of staff/student/parent has given clear consent for the Academy to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for the member of staff's employment contract or student placement contract.
(c) Legal obligation: the processing is necessary for the Academy to comply with the law (not including contractual obligations)

The members of staff responsible for data protection are mainly Mr P Wilson (Headteacher) and Mr C Fenton (Academy Data Protection Officer). However, all staff must treat all student information in a confidential manner and follow the guidelines as set out in this document.

The Academy is also committed to ensuring that its staff are aware of data protection policies, legal requirements and that adequate relevant training is provided to them. The requirements of this policy are mandatory for all staff employed by the Academy and any third party contracted to provide services within the Academy.

Notification:

Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register.

Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Personal and Sensitive Data:

All data within the Academy's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance: remove this link *https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/*

The principles of the Data Protection Act shall be applied to all data processed:

- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Fair Processing / Privacy Notice:

We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and students prior to the processing of individual's data.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'children' under the legislation.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/

There may be circumstances where the Academy is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example local authorities, 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 our Academy shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of individual's data shall first be notified to them.

Under no circumstances will the Academy disclose information or data:

- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the student in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the Academy or a local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another Academy or any other place of education and training, the child's potential employer, or any national body concerned with student admissions, without prior consent.

Data Security:
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them.

Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and where required these organisations shall provide evidence of the competence in the security of shared data.

Data Access Requests (Subject Access Requests):

All individuals whose data is held by us, has a legal right to request access to such data or information about what is held. We shall respond to such requests within one month and they should be made in writing to:

Mr P Wilson
Headteacher
Droylsden Academy
Manor Road
Droylsden
Manchester
M43 6QD

No charge will be applied to process the request.

Personal data about students will not be disclosed to third parties without the consent of the child's parent or carer, unless it is obliged by law or in the best interest of the child. Data may be disclosed to the following third parties without consent:

Other schools:

If a student transfers from Droylsden Academy to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.

Examination Authorities:

This may be for registration purposes, to allow the students at our Academy to sit examinations set by external exam bodies.

Health Authorities:

As obliged under health legislation, the Academy may pass on information regarding the health of children in the Academy to monitor and avoid the spread of contagious diseases in the interest of public health.

Police and Courts:

If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.

Social Workers and Support Agencies:

In order to protect or maintain the welfare of our students, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.

Educational Division:

Schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Right to be forgotten:

Where any personal data is no longer required for its original purpose, an individual can demand that the processing is stopped and all their personal data is erased by the Academy including any data held by contracted processors.

Photographs and Video:

Images of staff and students may be captured at appropriate times and as part of educational activities for use in the Academy only. Unless prior consent from parents/students/staff has been given, the Academy shall not utilise such images for publication or communication to external sources. It is the Academy's policy that external parties (including parents) may not capture images of staff or students during such activities without prior consent.

Location of Information and Data:

Hard copy data, records, and personal information are stored out of sight and in a locked storage area. The only exception to this is medical information that may require immediate access during the school day. This will be stored securely by the Student Services Manager.

Sensitive or personal information and data should not be removed from the Academy, however the Academy acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have off-site meetings, or are on school visits with students.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or student files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or student by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.

- If information is being viewed on a PC or laptop, staff must ensure that the window and documents are properly shut down and that the computer is locked before leaving it unattended. Sensitive information should not be viewed on public computers.
- If data needs to be accessed when away from the Academy, it should be done using a designated staff laptop via the secure remote access facility via the Academy website.
- If it is necessary to transport data away from the school, it should wherever possible be done using a secure staff laptop.
- If data is downloaded onto a USB stick or like device, it should not be transferred from this stick onto any home or public computers. Work should be edited from the USB, and saved onto the USB or a staff laptop only.
- USB sticks and other portable storage devices that staff use must be encrypted (password protected) in a way approved by the Academy IT Manager.

These guidelines are clearly communicated to all school staff, and any person who is found to be intentionally breaching this conduct will be disciplined in line with the seriousness of their misconduct.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk.

All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services.

All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/media/for-organisations/documents/1570/it_asset_disposal_for_organisations.pdf

The school has identified a qualified source for disposal of IT assets and collections.

The school also uses Shred-it to dispose of sensitive data that is no longer required.