Zest Academy Trust

Data Protection Policy

Approved by Trust Board: 19 June 2018
Review Period: Biennial
Policy Date Last Reviewed: 07/10/2020
Person Responsible: COO
Version Number: 2

Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 E admin@zestacademytrust.co.uk W www.zestacademytrust.co.uk

CEO Mark Hamblett

Introduction

The General Data Protection Regulation (GDPR) came into force on 25th May 2018 and as such all organisations within the European Union (EU) have a legal duty to ensure compliance.

The regulation provides a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed, retained, deleted or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration and disclosure.

Definitions

Data subject

An individual about whom such personal data relates to.

Data controller

The data controller is the body who is responsible for storing and controlling the personal data. Zest Academy Trust is the Data Controller.

Data processor

A data processor is responsible for processing personal data on behalf of a controller. There is a requirement to maintain records of personal data and processing activities, this includes but is not limited to: amending, retrieving, using, disclosing, erasing or destroying data.

Personal data

Personal data is information relating to an individual where they can be identified directly or indirectly. In particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to an individual.

Special category data

Special categories of personal data refer to an individual data subject's, race, ethnic origin, political view, religion, trade union membership, genetics, biometrics, health, sex life or sexuality.

Data Protection Principals

The data protection principals in accordance with the legislation are as follows:

1. Personal data must be processed lawfully, fairly and in a transparent manner
2. Personal data must be processed for a specific, explicit and legitimate purpose
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is being processed
4. Personal data must be accurate and, where necessary, kept up to date
5. Personal data must only be kept for as long as it is necessary for the purpose for which the data is processed
6. Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

Sharing personal data

The Trust will not share personal data with third-parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party:

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the Trust/Academy is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for

example, the local authority, 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 Trust/Academy shall be clearly defined within written notifications and details and basis for sharing that data given.

Transfer of Data outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.
The Trust/Academy will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the Trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Lawful Processing

The legal basis for processing data will be identified and documented prior to data being processed.

Under the GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Compliance with a legal obligation.
- The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- For the performance of a contract with the data subject or to take steps to enter into a contract.
- Protecting the vital interests of a data subject or another person.
- For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject unless reliance on consent is prohibited by EU or Member State law.
- Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former

members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.

- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
    - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.
    - Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

Consent

Where the Trust relies on consent as a condition for data processing then certain criteria must be adhered to. Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Consent must be a positive indication, it cannot be inferred from silence, inactivity or pre-ticked boxes. Where consent is given, a record will be kept documenting how and when consent was given.

Consent can be withdrawn by the data subject at any time.

Article 13 of the GDPR outlines the rights of individuals under the regulation:

- The right to be informed
- The right of access
- The right to rectification
- The right of erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

The right to be informed

The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge. If services are offered directly to a child, the Trust will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, and where applicable, the controller's representative and the DPO
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.
- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
    - Withdraw consent at any time.
    - Lodge a complaint with a supervisory authority.
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.

Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided.

Where data is not obtained directly from the data subject, information regarding the source the personal data originates from and whether it came from publicly accessible sources, will be provided.

For data obtained directly from the data subject, this information will be supplied at the time data is obtained. In relation to data not obtained directly from the data subject, this information will be supplied:

- Within one month having obtained the data
- If disclosure to another recipient is envisaged, at the latest, before the data is disclosed
- If the data is used to communicate with the individual, at the latest, when the first communication takes place

The right of access

Individuals have the right to obtain confirmation that their data is being processed and have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.
The Trust will verify the identity of the person making the request before any information is supplied. A copy of the information will be supplied to the individual free of charge; however, the Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

Where a SAR has been made electronically, the information will be provided in a commonly used electronic format. If a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. Upon receipt of a SAR a response will be issued without delay and at the latest, within one month of receipt

All fees will be based on the administrative cost of providing the information.

In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning

behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

The right to rectification

Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where the personal data in question has been disclosed to third parties, the Trust will inform them of the rectification where possible. Where appropriate, the Trust will inform the individual about the third parties that the data has been disclosed to.
Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex. Where no action is being taken in response to a request for rectification, the school will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to erasure

Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.
Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation

The personal data is processed in relation to the offer of information society services to a child
The Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes

- The exercise or defence of legal claims

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

The right to restrict processing
Individuals have the right to block or suppress the Trust's processing of personal data.
In the event that processing is restricted, the Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

The Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead

Where the Trust no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim. If the personal data in question has been disclosed to third parties, the Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The Trust will inform individuals when a restriction on processing has been lifted.

The right to data portability
Individuals have the right to obtain and reuse their personal data for their own purposes across different services. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

Personal data will be provided in a structured, commonly used and machine-readable form. The Trust will provide the information free of charge. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations. In the event that the personal data concerns more than one individual, the Trust will consider whether providing the information would prejudice the rights of any other individual. The Trust will respond to any requests for portability within one month.

Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request. Where no action is being taken in response to a request, the Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

The right to object

The Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

Where personal data is processed for direct marketing purposes:

- The Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes

Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.

Where the processing activity is outlined above, but is carried out online, the Trust will offer a method for individuals to object online.

Automated decision making and profiling

Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling
- It produces a legal effect or a similarly significant effect on the individual

The Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
When automatically processing personal data for profiling purposes, the Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.

- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law

Accountability

The Trust will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The Trust have taken the following steps to ensure and document GDPR compliance:

Data Protection Named Contact for the Trust

Mrs Nicola Lea COO (Chief Operations Officer)
Nicola.Lea@zestacademytrust.co.uk

Data Protection advisors
DPOservice@schoolspeople.co.uk

The appointed DPO will be responsible for:

- Informing and advising the Trust and its employees about their obligations to comply with the GDPR and other data protection laws.
- Monitor the Trust's compliance with the GDPR and other legislation, including managing internal data protection activities, advising on data protection impact assessments (DPI), conducting internal audits and providing the required training to staff members
- Ensuring that there is no conflict of interests in undertaking the DPO role
- Operating independently and will not be disciplined or penalised for performing the duties of the DPO

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Personal data breaches

The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.
The GDPR requires the Trust to notify any applicable personal data breach to the information Commissioner's Office (ICO).

The Trust have put in place procedures to deal with any suspected personal data protection breach and will notify data subjects or any applicable regulator where we are legally required to do so. If you know or suspect a personal data breach occurred, then you must report the data breach immediately through the Trusts online reporting mechanism. Within a breach notification the following information should be include:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

If the risk is classed as 'high risk' then the individual or individuals take priority and should be notified prior to the authorities. If the breach is sufficiently serious, the public will be notified without undue delay.

Privacy by design

The Trust will act in accordance with the GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Trust has considered and integrated data protection into processing activities.

Data impact assessments (DPIAs)

In order to achieve a privacy by design approach the Trust conducts DPIAs for all new technologies or programmes being used by the Trust which could affect the processing of personal data. DPIAs will be used to identify the most effective method of complying with the Trust's data protection obligations and meeting individuals' expectations of privacy.

DPIAs will allow the Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Trust's reputation which might otherwise occur. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV

The Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals
- The measures implemented in order to address risk

Where a DPIA indicates high risk data processing, the Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

Record keeping

The Trust are required to keep full and accurate records of data processing activities. These records include:

- Name and contact details of the Trust
- Name and contact details of the DPO
- Descriptions of the types of personal data used
- Description of data subjects
- Details of the Trusts data processing activities and purposes as outlined in the Trusts data asset register
- Details of any third-party recipients of the personal data
- Where personal data is stored
- How long data is retained for
- How the data is secured

Data security

- Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.
- Confidential paper records will not be left unattended or in clear view anywhere with general access.

- Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.
- Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use.
- Memory sticks will not be used within the Trust
- All electronic devices are password-protected to protect the information on the device in case of theft.
- Where possible, the Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
- Staff, Trustees and Academy Council Members will not use their personal laptops or computers for storing any Trust/Academy data
- All necessary employees are provided with their own secure login and password, and every computer regularly prompts users to change their password.
- Emails containing sensitive or confidential information will be password protected in a password protected document attachment
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
- Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the school premises accepts full responsibility for the security of the data.
- Before sharing data, all employees will ensure:
    - They are allowed to share it.
    - That adequate security is in place to protect it.
    - Who will receive the data has been outlined in a privacy notice.
- Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Trust/Academy containing sensitive information are supervised at all times.
- The physical security of the Trusts buildings and storage systems, and access to them, is reviewed on a termly basis. If an increased risk in vandalism/burglary/theft is identified, extra measures to secure data storage will be put in place.
- The Trust takes its duties under the GDPR seriously and any unauthorised disclosure may result in disciplinary action.

Monitoring

The Trust will monitor the effectiveness of all policies and procedures.

Related policies

The following policies are related to this data protection policy:

- data retention policy
- data breach policy
- working at home policy
- remote working policy
- disclosure and barring service storage policy
- privacy notices

These policies are also designed to protect persona data and can be found at www.zestacademytrust.co.uk