Zest Academy Trust

The Individual Rights of Data Subjects: Policy and Procedure

Approved & Adopted By Trust Board: 19/06/2018
Review Period: Annual
Policy Date Last Reviewed/Approved: 20/02/2023
Person Responsible: DPO
Version Number: 1

The Individual Rights of Data Subjects:Policy and Procedure

Contents

Zest Academy Trust, Waterloo Road, Blackpool, FY4 3AG
T 01253 315370 Registered in England No. 8087508

Policy Statement

Zest Academy Trust (hereafter the Trust) is committed to ensuring that its systems and processes support the rights of individuals in respect of their personal data and that as an organisation we can recognise and respond appropriately and effectively to individuals exercising their rights under Articles 12 – 22 of the UK GDPR.

Individual Rights of Data Subjects

The Data Protection Policy sets out the broad organisational and staff requirements relating to data protection legislation.

This document explains the rights of individual data subjects whose data the Trust may process and the procedures it will follow to ensure those rights are met.

The Rights

Under data protection legislation, a person whose data we hold has several rights, these are:

1. **The right to be informed** – being told about the type of information we collect and how we use and look after it
2. **The right of access (Subject Access Requests)** – being given a copy of the personal data we hold about the individual
3. **The right to rectification** – having inaccurate personal data corrected
4. **The right to erase (the right to be forgotten)** – having personal data deleted from records or records deleted entirely
5. **The right to restrict processing** – requiring us to store but not use personal data concerning the individual
6. **The right to data portability** – being provided with an electronic copy of certain records to use for a different purpose
7. **The right to object** – to put a case forward for stopping processing including marketing
8. Rights concerning **automated decision making and profiling** – to have a human reconsider automated decisions and profiling
9. **The right to withdraw consent**

The Legislation

This document is based on the requirements of the UK General Data Protection Regulation, The Data Protection Act 2018, and the guidance of the UK Information Commissioner.

The legislation applies to personal information relating to living individuals who can be identified from it. This may be automatically processed information held on the Trust's computer systems, as well as information in our structured manual records, such as paper files.

It also applies to CCTV recordings, photograph, video and audio recording

Management of Requests

The Trust will maintain a record of all data subject rights requests. A tracking tool for the management of requests is enclose in Appendix 1.

Data subjects may make rights requests verbally or in writing including through social media channels. It is the Trust's responsibility to ensure its staff recognise a data subject rights request and that that are familiar with reporting lines to ensure the request is verified and actioned within the statutory timescales.

A record of data subject rights requests received will be maintained by the Trust.

Support with interpretation of the legislation, guidance and management of requests may be sought from the Data Protection Officer Service.

The Trust's Data Protection Officer can be reached by emailing

DPOService@schoolspeople.co.uk

The Rights in Detail

The following sections explain the rights in detail and how they should be applied.

The Data Protection Officer will offer advice and support in the practical application of these rights.

The Right to be Informed

The legislation requires the Trust to be transparent about how it processes personal data. It must clearly explain how we collect, store and use the personal data individuals entrust to us. We do this by providing Privacy Notices, sometimes referred to as 'fair processing notices'.

The legislation sets out the information that should be included in a Privacy Notice and when individuals should be informed. The point of notification is determined by whether the personal data is collected directly from individuals or a third party.

The table below summarises the information we should supply to individuals and at what stage.

What information must be supplied?	Data obtained directly from the data subject	Data obtained from a third party
Identity and contact details of the data controller and the data protection officer	✓	✓
Purpose of the processing (what we need to do with the data) and the lawful basis for the processing (what we are legally allowed to do with the data)	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data	✓	✓
Any recipient or categories of recipients of the personal data (who we may share the data with)	✓	✓
Details of transfers to third countries and safeguards	✓	✓
Retention period or criteria used to determine the retention period (how long we will keep the data)	✓	✓
The existence of each right of data subjects	✓	✓
The right to withdraw consent (for processing) at any time, where relevant	✓	✓
The right to complain to the supervisory authority (the Information Commissioner)	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓

Whether the provision of personal data is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data	✓	
The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should the information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month)
		If the data are used to communicate with the individual, at the latest, when the first communication takes place; or
		If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

The information supplied must be:

- Concise, transparent, intelligible and easily accessible
- Written in clear and plain language, particularly if addressed to a child; and
- Free of charge

When drafting and updating Privacy Notices, the Trust will follow the ICO's guidance regarding the

‘right to be informed’.

Responsibility for privacy notices

It is the responsibility of the Trust as Data Controller to ensure that adequate information is provided to individuals regarding the processing of their data.

Support with the production of suitable Privacy Notices may be sought from the Data Protection Officer.

Once finalised, Privacy Notices will be published on the Trust’s website.

The Right of Access (Subject Access Requests)

Individuals have the right to access their personal data and other supplementary information stipulated under the UK GPDR. This allows individuals to be aware of and verify the lawfulness of the way in which their data is being processed.

Most commonly, individuals simply want to be given a copy of the information held about them. However, under data protection legislation, individuals also have the right to obtain:

- confirmation that their data is being processed
- other supplementary information (similar to the information provided in a privacy notice – see above)

This is known as a Subject Access Requests (SAR). A request may be made verbally or in writing including via social media channels. All staff should be aware that any request for personal data may be a subject access request and should be treated as such until proven otherwise.

Charging for information

A copy of the requested data must be provided free of charge, with the exception that a ‘reasonable fee’ may be charged when a request is deemed ‘manifestly unfounded or excessive’.

A fee may also charge to comply with requests for further copies of the same information.

The fee must be based on the administrative cost of providing the information.

Time constraints

The information must be provided without delay and at the latest within:

- one calendar month of receipt of a valid SAR for standard requests
- three calendar months of receipt of a valid SAR where requests are complex or numerous BUT ONLY if we inform the individual within one month of the receipt of

the request and explain why the extension is necessary.

A SAR is valid when we are satisfied with the identity of the requester and their entitlement to access the requested data.

Verifying the identity of the requestor

The identity of the person making the request must be verified, using 'reasonable means' to ensure personal data is not inadvertently released to a third party who is not entitled to it.

The Trust may, where it is unable to reliably verify the identity of the requester via **its** records, request evidence of identity as follows:

(a) Photographic Confirmation:

- full driving licence, passport,

(b) Confirmation of name and address:

- full driving licence, utility bill, bank or credit card statement or another equivalent/similar official document –it MUST show the Requesters name and address).

Refusing a request

Where requests are deemed manifestly unfounded or excessive rather than charge a fee, we may refuse to respond.

Where we refuse to respond to a request, we will without undue delay and at the latest within one calendar month:

- Explain to the individual why we will not respond to their request,
- Inform them of their right to complain to the Information Commissioner and a judicial remedy.

The format in which data is to be provided

If an individual makes a request electronically, the data should be provided in a commonly used electronic format, unless the individual requests otherwise.

Where codes have been used within the data, for example, student attendance data, the code key must be provided to ensure the requestor fully understands the data

Third party data

This right to access personal data should not adversely affect the rights and freedoms of others.

The obligation is to provide information rather than documents. The Trust may redact third-party data and/or edit any information that is outside the scope of the access request

If this is not possible, the Trust does not have to comply with the request except where:

- the other individual/s consents to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

Exemptions and restrictions

In some circumstances, we may have a legitimate reason for not complying with a Subject Access Request. The Data Protection Act 2018 (Schedule 2 & 3) sets out several exemptions from the duty to do so.

This may mean that we refuse to provide all or some of the information requested under these exemptions.

For further information please see here

The Right to Rectification

The Trust has an obligation under data protection legislation to ensure that the information we hold about individuals is accurate and complete. If an individual believes that the information we hold is inaccurate or incomplete, they have the right to ask for the data to be amended.

On receipt of a request, the Trust must decide whether or not it agrees that the data is inaccurate or incomplete.

There may be occasions when data may have been correct at the time it was recorded but later found to be inaccurate, for example, a medical diagnosis which is later superseded by a different diagnosis. It will not always be appropriate in instances such as these to delete data, it might be more appropriate to ensure that the record is clear about what has happened.

Similarly, a record of an opinion may be an accurate record of that opinion, even if that opinion is wrong.

Requests for rectification will be considered in line with guidance on the subject from the ICO. Support with interpreting the guidance may be sought from the Data Protection Officer.

While considering a request for rectification it may be necessary to ***restrict*** the use of the contested data (see the right to restrict processing, below). Systems and records will be noted as being 'in dispute' until enquiries have been completed.

Timescale for response

A response must be provided to the requestor within:

- one month of receipt for standard requests
- three months of receipt where the request for rectification is complex

If data is decided to be inaccurate, methods of rectification include the incorrect data being amended, struck through or erased. Where necessary a clear note will explain the reason for the rectification the note should contain details of who made the change and the senior manager/administrator who authorised the change.

Where the Trust are:

- taking rectification action, and the incorrect/incomplete data has been disclosed to third parties, the third parties must be informed of the rectification where possible. The requestor must also be informed of any third parties to whom the data has been disclosed.
- are not taking action in response to the rectification request, we must explain why and inform the requester of their right to complain to the Information Commissioner and a judicial remedy.

The Right to Erasure ('the right to be forgotten')

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for the Trust to process it.

The Trust can refuse to comply with a request for erasure in certain circumstances including where the processing is necessary:

- to comply with a legal obligation
- for the performance of a public interest task, or the exercise of official authority
- Erasure may be requested where:
- consent is the only lawful basis for processing and that consent is withdrawn
- legitimate interests are the lawful basis for processing, and there is no overriding legitimate interest to continue the processing (The Trust may not rely on this lawful basis for processing carried out in its official capacity)
- the personal data is no longer necessary for the purpose for which it was originally processed

- the processing is for direct marketing purposes
- the data is processed unlawfully
- erasure is required under a legal obligation
- the data has been processed to offer information society services to a child.
- For more information on the right to erasure please see Right to erasure | ICO

Deciding whether the right applies

The right to erasure does not provide an absolute 'right to be forgotten'. There are some specific circumstances where the right to erasure **does not apply,** and the Trust can refuse the request, including where the data is processed:

- 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
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- for the exercise or defence of legal claims.

Each request for erasure will be considered on its merits and in line with ICO guidance.

Applications relating to children's data

There are extra requirements when the erasure request relates to the personal data of a child.

Special attention must be given to situations where a child has given consent to processing and later request the erasure of the data. This is because a child may not have been fully aware of the risks involved in the processing at the time of consent. Guidance from the Information Commissioner's Office will be followed in relation to any such requests.

Informing other organisations about the erasure of personal data

Where the Trust has:

- decided to erase data and where the data has previously been disclosed to third parties. Those third parties must be informed about the erasure of the personal

data unless it is impossible or involves a disproportionate effort to do so.

- made the personal data public, for example on social networks, or websites the data should be removed.

Timescale for action

Legislation requires that erasure be carried out 'without undue delay' and within one calendar month.

The Right to Restrict Processing

Individuals have a right to 'block' or suppress the processing of personal data.

When processing is restricted, the Trust are permitted to securely store the personal data, but no further processing is permitted.

Restriction of processing is required in the following circumstances:

- when considering a request for data rectification, erasure (see above) or an objection to processing (see below).
- when processing is unlawful, and the individual opposes erasure and requests restriction instead (they don't want their data to be completely erased)
- where the personal data is no longer required but the individual requires it to establish, exercise or defend a legal claim

How do we restrict processing?

The Trust should have processes in place that enable the restriction of personal data if required. The UK GDPR suggests several different methods that may be used to restrict data, including:

- temporarily moving the data to a secure storage system
- making the data unavailable to users (use of access controls); or
- temporarily removing published data from a website.

The Trust must consider how to securely store personal data that is no longer required but the individual has requested restriction (effectively requesting the data is not erased).

For more information on the right to restrict processing please see Right to restrict processing | ICO

Informing other organisations about the restriction of personal data

Where the personal data has been disclosed to third parties, they must be informed about the restriction on the processing unless it is impossible to do so or involves disproportionate effort.

The requester must be informed when the Trust decides to lift a restriction on processing.

The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

It allows them to move, copy or transfer personal data easily from one IT environment to another safely and securely, without hindrance to usability.

When does the right to data portability apply?

The right to data portability only applies:

- to personal data the individual has provided to the Trust
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means (electronic, not paper records)

The conditions are cumulative, and all must be met for a request for portability to be successful. Each request will be considered on its merits.

For more information on the right to data portability please see Right to data portability | ICO

Responding to a request

When a request meets the criteria for data portability, the Trust must provide the personal data in a structured, commonly used and machine-readable format.

Commonly used open formats include CSV, XML, JSON. Other formats exist that also meet the requirements of data portability.

If the individual requests it, the Trust may be required to transmit the data directly to another organisation (if this is technically feasible). However, the Trust are not required to adopt or maintain processing systems that are technically compatible with other organisations.

If the personal data concerns more than one individual, we must consider whether providing the information would prejudice the rights of any other individual.

Timescale

The Trust must respond without undue delay, and within one calendar month of receipt of a request.

The timescale may be extended by two months when the request is complex, or several requests are received. The individual must be informed of the extension to the timescale together with an explanation of why the extension is necessary.

Where the request is refused, the individual must be informed without undue delay and at the latest within one month of receipt. The refusal notice must include:

- the reason why the Trust are not taking action,
- their right to complain to the Information Commissioner and a judicial remedy

The Right to Object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Personal data processed for the performance of a legal task or legitimate interests

Individuals are required to base their objection on “grounds relating to their particular situation”.

The Trust must stop processing the personal data unless:

- it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims

Individuals must be informed of their right to object “at the point of first communication” and in Privacy Notices The right must be explicitly brought to the attention of the data subject and be presented clearly and separately from any other information.

Personal data processed for research purposes

Individuals must have “grounds relating to his or her particular situation” to exercise their right to object to processing for research purposes.

If the Trust is conducting research where the processing of personal data is necessary for the

performance of a public interest task, it is not required to comply with an objection to the processing.

Personal data processed for direct marketing

The factors that are used to identify direct marketing material are:

- Directed to particular individuals – addressed/directed to a particular person.
- Communication by whatever means - includes all means by which the Trust might contact individuals, such as letters, emails and text messages.
- Advertising or marketing material - Direct marketing includes promoting particular views or campaigns, such as those of a charity. If the Trust are using personal data to elicit support for a good cause, it is still carrying out direct marketing.

Requests to stop direct marketing

The right to object to direct marketing is absolute. Direct marketing activity must cease as soon as the as soon as Trust receive an objection. There are no exemptions or grounds to refuse.

The Trust:

- must inform individuals of their right to object “at the point of first communication” and in its Privacy Notices.
- must deal with an objection to processing for direct marketing at any time and free of charge

The Trust is not required to respond to a notice to stop direct marketing – it only requires immediate cessation. However, acknowledging receipt and confirming the Trust has acted on the objection is good practice, where this is appropriate

Timescale for response

Direct marketing must stop immediately after an objection is received. The ICO recognises that a particular marketing campaign might already be underway when a notice is received and that the individual may subsequently receive further marketing material.

However, the ICO expects that in normal circumstances electronic communications should stop within 28 days of receiving the notice, and postal communications should stop within two months.

Rights Related to Automated Decision-Making and Profiling

Automated individual decision-making is a decision made by automated means with no human involvement in the decision-making process. Where this type of decision-making takes place,

individuals have the right to request that important decisions taken by us based on their personal information have some sort of human input.

The Trust does not use automated decision-making or profiling in any of its processing activities.

The Rights Related to Withdraw Consent

The right to withdraw consent applies where consent is the only lawful basis for processing.

This right is absolute. As soon as Trust receives a withdrawal of consent the processing should cease at the earliest opportunity. There are no exemptions or grounds to refuse this right.

Trust must inform individuals of their right to withdraw consent "at the point of first communication" and in its Privacy Notices.

Acknowledging receipt of the withdrawal of consent and confirming the Trust has acted on the withdrawal is good practice, where this is appropriate.

Legal Consequences of a Failure to Comply with Individual Rights

Anyone who believes they are directly affected by the processing of personal data may ask the Information Commissioner's Office (ICO) to assess whether it is likely or unlikely that such processing complies with the legislation.

If the ICO's assessment shows that it is likely that the Trust has failed to comply, they may ask it to take steps to comply with the data protection principles. Where appropriate, the ICO may order it to do so. The ICO has no power to award compensation to individuals – only the courts can do this. Therefore, judicial action may follow.

The Information Commissioner may serve an enforcement notice if they are satisfied that the Trust have failed to comply with the individual rights of data subjects. An enforcement notice may require the Trust to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence.

The Information Commissioner has the statutory power to impose a financial penalty on an organisation if they are satisfied that the organisation has committed a serious breach of the Data Protection Act (2018) that is likely to cause substantial damage or distress.

Appendix 1. DSR Request Management and Record

Internal Use Only: Attach all relevant documents relating to the DSR request and fulfilment

Category of DSR Request Received

Right of Access (Subject Access Request)	
Right to Rectification	
Right to Erasure (Right to be Forgotten)	
Right to Restrict Processing	
Right to Data Portability	
Right to Object to Processing	
Right to Withdraw Consent	

Section 1: DSR Details			
DSR Received	*Form/Email/ Letter/Verbal/ Other*	*Date Received*	
DSR Form Received	*Yes / No*	*DSR Form Signed*	*Yes / No*
ID Docs enclosed?	*Yes / No*	*ID Valid*	*Yes / No*
ID verified on systems by *(name & position)*			

Section 2: Further verification required			
Identity verification required	*Yes / No*	*Date ID verification requested* *(Attach copy to this record)*	
Address Verification required	*Yes / No*	*Date address verification requested*	
Identity Confirmation Received	*Yes / No*	*Date Received*	
Address confirmation received	*Yes / No*	*Date Received*	
ID verified on systems by *(name & position)*			

Section 3: Third-Party Consent			
Third-party request	*Yes/No*	*Third-party consent required?*	*Yes/No*
Third-party consent enclosed?	*Yes/No*	*Date third party consent requested* *(Attach a copy to this record)*	
Date 3rd party consent received		*3rd party consent valid*	*Yes/No*
3rd party consent verified by *(name & position)*			

Section 4: Request Validation			
Rights Request valid?	*No*	*Date Refusal Notice sent. (Attach a copy to this record)*	
	Yes	*Date Acknowledgment sent (Attach a copy to this record)*	

Section 5: SAR Data Management			
Data Identification allocated to		*Date Completed*	
Redacting allocated to		*Date Completed*	
Supplementary Data Compiled by		*Date Completed*	
Fulfilment letter drafted by		*Date Completed*	

Notes: