Data Subject Right to Restriction Policy

Version Number	V1.1
Approved on	7th November 2025
Last Version	N/A New Policy
Approved on	N/A
Approved By	Board of Trustees

Change Record

Version No	Date of Change:	Changed By:	Comments:

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

Under the GDPR and Data Protection Act 2018, individuals have the right to request the restriction or suppression of the processing of their personal data. This is not an absolute right and only applies in certain circumstances. When processing is restricted, it is permissible to store the personal data but not to use it.

What must I do?

1. **MUST:** Staff must recognise when a data subject, or a data subject's representative has made a request for the processing of their data to be restricted or suppressed. The request can be made verbally or in writing, including via social media. It is usual that this policy will come into force once a data subject exercises their right to object to the processing of their data or requests rectification of their data, please also see the Data Subject Right to Rectification Policy and Data Subject Right to Object Policy;
2. **MUST:** Staff must recognise that a third party can make a request for data processing to be restricted or suppressed on behalf of another person;
3. **MUST:** Requests for the processing of information to be restricted or suppressed should be provided free of charge, however, where requests are repetitive or excessive, the data controller or processor is permitted to make reasonable charges for the information. Repetitive and excessive requests must be reported to the CEO;
4. **MUST:** Requests must be responded to without delay and within one month of receipt of the request. If the request is complex, or if a number of requests are received from one data subject, this may be extended by a further two months;
5. MUST: We must have appropriate methods in place to restrict the processing of personal data on our systems;
6. MUST: We have have appropriate methods on our systems to indicate that further processing has been restricted;
7. MUST: We must understand the circumstances when we can process personal data that has been restricted;
8. MUST: We must have procedures in place to inform any recipients of the data that the processing has been restricted;
9. MUST: Once a request has been received, follow the steps in the Data Subject Right to Restriction Procedure

Why must I do it?

1. Staff must recognise and act upon a request by a data subject's request to restrict or suppress processing of their data to adhere to the GDPR and Data Protection Act 2018. Failure to do so may result in fines and reputational damage. It is also important that staff use this policy once a request for rectification or objection has been received from an individual;
2. Staff must be aware that a third party can request the restriction or suppression of processing personal data on behalf of another person in order to adhere to the GDPR and Data Protection Act 2018, for example in the case of children.
3. Under the GDPR and Data Protection Act 2018, data subjects have the right to request restriction or processing of their data without charge. The exception to this is where requests are repetitive or excessive in nature. The CEO has the overall decision on whether a request is excessive or repetitive and charges must not be made without consultation.
4. Staff must be aware that the deadlines are set in law and must be adhered to. Failure to do so may result in fines and reputational damage.
5. When a data subject requests that the processing of their data is restricted or suppressed, they are effectively requesting that the data is stored and not erased and that no further processing takes place. This could be for reasons that the data subject is challenging the accuracy of their data (please also see Data Subject Right to Rectification Policy), or that the data subject believes their data has been processed unlawfully, or that the data subject requires that the data is kept to exercise or defend a legal claim, or that the data subject has objected to the processing of their personal data under article 21(1) and consideration is being given to whether the legitimate grounds of Essex & Thames override those of the individual. Please also see Data Subject Right to Object Policy. Systems must allow that all further processing can be restricted or suppressed.
6. To be able to comply with this policy and the UK GDPR methods must be in place to ensure that the request to restrict or suppress data is upheld where this right has been assessed as overriding the legitimate interests of Essex & Thames Education.
7. It may not always be possible to completely restrict processing of personal data for reasons such as audits and inspections. However, where this is the case, only the minimum amount of processing in order to fulfill the obligation will be permitted.
8. Data subjects must be kept informed of the progression of their request and advised of the action taken as soon as possible.
9. Following the Data Subject Right to Restriction Procedure will ensure that the obligations of Essex & Thames Education under the UK GDPR and this policy are met.

How must I do it?

For all requests, staff must refer to the Data Subject Right to Restriction Procedure as soon as a request to restrict or suppress processing of personal data is received.

The Record of Processing Activities (ROPA), should be updated, with all actions logged as the process continues.

What if I need to do something against the policy?

If you believe you have a valid business reason for an exception to these policy points, having read and understood the reasons why they are in place, please raise a formal request by contacting Sue Rudgley (DPO - sue@ete.org.uk)

Breach Statement

Breaches of Information Policies will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Further Information

For further reading and information, please visit the ICO website page for Subject Access Requests by following the link below:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-restrict-processing/

Key Contacts

Data Protection Officer (DPO):
Sue Rudgley
sue@ete.org.uk
01268 988580 ext 1000

Senior Information Risk Officer (SIRO)
Jo Palmer-Tweed
jo@ete.org.uk

Information Commissioner's Office (ICO)
https://ico.org.uk/global/contact-us/contact-us-public/