Data Subject Right to Object Policy

Version No	V1.1
Approved on	7th November 2025
Previous Version No	N/A New Policy
Approved on	N/A
Approved By	Board of Trustees

Change Record

Date of Change:	Changed By:	Comments:
28/05/2025	Sue Rudgley	New Policy

The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being processed for direct marketing purposes. This policy is closely linked to the Data Subject Right to Restriction Policy.

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

What must we do?

1. **MUST:** All employees, Trustees, Committee Members and Self Employed Staff must comply with the requirements of the UK GDPR, the Data Protection Act 2018 and Article 8 of the Human Rights Act when processing the personal data of living individuals;
2. **MUST:** We must know how to recognise an objection and understand when the right applies;
3. **MUST:** We must record all requests, including those that are received verbally;
4. **MUST**: We must understand when we can refuse a request and be aware of the information we need to provide to individuals when refusing a request;
5. **MUST:** We must have a process in place to ensure that we respond to the objection without undue delay and within one month of receipt;
6. **MUST:** We must be aware of the circumstances when we can extend the time limit to respond to a request;
7. **MUST:** We must have appropriate methods in place to erase, suppress or otherwise cease processing information;
8. **MUST:** We must have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights;
9. **MUST:** We must understand when we need to inform individuals of their right to object in addition to including it in our privacy notice.

Why must we do it?

1. We must abide by the laws set under the UK GDPR and Data Protection Act 2018. Failure to do so can result in not only financial penalties but in reputational damage and loss of trust in the organisation;
2. Individuals have the right to object to the processing of their personal data under the UK GDPR and Data Protection Act 2018. It is important that objections, in any format are recognised so that they can be actions within the deadline of one month from the date of request;
3. A record of all requests must be held in order to effectively track and manage requests from individuals;
4. It is not always possible to erase, suppress or otherwise cease processing data, some data must be kept for reasons such as for the performance of a task in the public interest or complying with a legal obligation;
5. We must ensure that all requests are responded to within one month of receipt and fully tracked to completion to meet our obligations under the UK GDPR and Data Protection Act 2018.
6. More complex requests may require additional time and we must follow procedure when extending the time to respond to ensure that the data subject is aware of the extension and the reasons for this;
7. We must have systems in place to effectively erase, suppress or otherwise cease processing data where the objection to processing is upheld as we cannot continue to store or process the data in circumstances where the objection is justified;
8. Individuals must be informed of their rights under the GDPR and Data Protection Act 2018 and these must be clearly stated in our privacy notice;
9. It must be easy for individuals to access information about their rights in relation to their personal data.

How must we do it?

1. We must follow the data protection policy and related policies and procedures to ensure we meet our obligations under the UK GDPR and Data Protection Act 2018;
2. We must recognise that an individual can object to their data being processed in any format, including verbally and in writing, including email and social media channels. The request must be passed onto the DPO without delay, please see the Data Subject Right to Erasure Procedure;
3. We must follow the Data Subject Right to Erasure Procedure by logging all requests on the 'Erasure Request' tab on the ROPA;
4. By following the Data Subject Right to Erasure Procedure we can determine if the request for erasure is valid and follow the procedure to either complete or refuse the request;
5. By following the Data Subject Right to Erasure Procedure we can ensure that we are responding to the request within the timeframe of one month from the date of the request;
6. The Data Subject Right to Erasure Procedure provides guidance on when a request can be extended past one month from the date of the request for erasure and the steps to be taken;
7. The Data Subject Right to Erasure Procedure provides the process for ensuring that all data is erased where the request has been upheld.

Roles and Responsibilities:

Data Protection Officer:	Sue Rudgley sue@ete.org.uk 01268 988580 ext 1000
Senior Information Risk Officer:	Jo Palmer-Tweed jo@ete.org.uk 07530 184210

Advice and Support

If you require any further information then please contact 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.