Data Sharing Policy for Third Parties

Version No	V1.2
Approved on	26th March 2026
Previous Version No	N/A New Policy
Approved by	Board of Trustees
Version No	V1.1

Change Record

Date of Change:	Changed By:	Comments:
17/10/2025	Sue Rudgley	New Policy
31/12/2025	Sue Rudgley	Added point 14 - Requirement to review data sharing

General rules in complying with Data Protection law

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

What must we do?

Data sharing for Third Party processors is separate and distinct from data sharing with third parties. This policy deals exclusively with sharing with third party processors that process data under the instruction of Essex & Thames Education. For data sharing with third parties (external organisations), please see our Data Sharing with Data Sharing Policy for Third Parties (External Organisations that are Controllers).

This policy should be referred to for engagements such as the auditors, the lecture team and the personal tutor team. Almost all sharing, other than the DfE and Ofsted will be covered by this policy.

1. **MUST:** We must understand the difference between data sharing with third parties and data sharing with third party processors;
2. **MUST:** We must have accountability for sharing the data;
3. **MUST:** We must show fairness and transparency when sharing data;
4. **MUST**: We must have a lawful reason for sharing the data;
5. **MUST:** We must have reasonable security measures in place when sharing data;
6. **MUST:** We must understand what is meant by data sharing;
7. **MUST:** We must advise organisations that we are the data controller and they are the data processor;
8. **MUST:** We must ensure that where we are routine sharing that this is for an established and clearly defined purpose;
9. **MUST:** We must justify an exceptional (one-off) sharing events;
10. **MUST**: We must consider if:
    a. There is a benefit to sharing;
    b. If sharing is necessary;
    c. If we are being fair and transparent;
11. **MUST:** We must have a clear and easy to obtain way for data subjects to make a complaint or to enquire about their data;
12. **MUST:** We must be clear on how we can share data in an emergency situation;
13. **MUST:** We must keep our policies and procedures for data sharing under regular review;
14. **MUST:** We must have a review process in place to examine if data sharing is still appropriate;
15. **MUST NOT:** You must not share any personal data held by us with an individual or organisation based in any country outside of the European Economic Area, unless appropriate adequacy agreements or the EU-U.S. Data Privacy Framework (EU-U.S. DPF) applies, in these circumstances, approval of the Board of Trustees should be sought with the assistance of the DPO. Only systems **approved** by the Board of Trustees should be used.
16. **BEST PRACTICE:** We should consider putting data sharing agreements in place

Why must we do it?

1. There is a distinct difference between data sharing with third parties and data sharing with third party processors. There must be a separate policy and procedures for each;
2. We must have accountability to comply with the UK GDPR and Data Protection Act 2018 to provide assurances that the data of individuals is kept safe, this in turn provides trust in our organisation. There must be:
    a. A legal reason for the data sharing;
    b. Consideration to the risks that data sharing may create;
    c. Training for staff on how to share data safely;
3. We must ensure that any sharing of personal data is:
    a. Reasonable, expected and made clear to data subjects.
    b. Treating individuals fairly and not using data in any unjust ways;
    c. Reasonable and proportionate;
    d. Expected by individuals;
4. 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. Data subjects have the right to understand how their data is used and shared;
5. We must take reasonable steps to ensure that data is shared and stored securely using appropriate security measures, this also applies to when data is shared externally;
6. To ensure that we meet the requirements of this policy, all staff must be aware of what data sharing is and the implications;
7. We must ensure that all parties understand their status in regard to data processing. For Third Party Processors, we are the data controller and they are the processor;
8. Where we are routinely sharing data, for example for an audit, we must have an established and clearly defined purpose;
9. Where sharing of data is exceptional (one off) we must have considered and be able to show justification for the sharing;
10. We must consider all sharing before commencing to do so, weighing up the risks and benefits before sharing commences and document our reasoning to stay compliant with data protection law;
11. Where we are sharing, there should be one point of contact for data subjects to be able to quickly and easily submit a complaint;
12. Where there is an emergency, it could be more harmful not to share data so it is essential that sharing is permitted to prevent potentially serious consequences;
13. To ensure that our policies and procedures still meet the requirements for sharing with the ICO Data Sharing Code of Practice;
14. To ensure that data sharing is still proportionate and appropriate;
15. To comply with the right of the Data Subject to have equivalent legal safeguards in place over their data in another country as they would here. The member states of the EEA share common legislation which provides assurance to us that personal data will be securely handled under the same provisions that exist under the Data Protection Act.

16. Although it is not compulsory to do so, consideration should be given to putting data sharing agreements in place as a matter of best practice.

How must we do it?

1. We must demonstrate that we understand the difference between Data Sharing with Third Parties and Data Sharing with Third Party Processors by holding a Data Sharing Policy for Third Parties and a Data Sharing for Third Party Processors Policy and by following the steps in the Data Sharing Procedure for Third Parties and the Data Sharing for Third Party Processors Procedure. Data sharing with third parties refers to sharing where the organisation or person that the data is being shared with has control on how that data is processed. Data sharing with third parties differs in that the organisation or person that the data being shared with works under the instruction of Essex & Thames Education;
2. We can demonstrate accountability by follow the points in this policy, reviewing and updating the Data Protection Accountability Tracker, following the Data Protection Policy and the Data Sharing for Third Party Processors Procedure:
    a. Our ROPA shows all data flows and provides the legal basis for processing and sharing data, the details are shown in our Privacy Notice;
    b. A DPIA will be carried out for any new sharing, checking the risk to individuals;
    c. Staff training is provided on an annual basis and wherever a need arises;
3. We can demonstrate that sharing is reasonable, fair, and expected by:
    a. Showing who we share data with in our ROPA and within our Privacy Notice;
    b. Ensuring that all staff are trained to only use data for the purpose for which is was collected and processed and shared in line with our ROPA and Privacy Notice;
    c. Considering when to share data that the reason is reasonable and proportionate, considering the specific aims, why it is necessary and the benefits to the individual or wider society;
    d. Ensuing that individuals are made aware of who their data is shared with;
4. There must be a lawful basis for for sharing data, this must be indicated on the DPIA and details added to the Data Sharing Records tab of the ROPA and provided on the Privacy Notice;
5. As part of the DPIA, we should agree on the security systems to be put in place when processing and storing the data. We can do this by following the points on the Data Sharing for Third Party Processors Procedure and ensuring a Third Party Contractor Data Processing Agreement is in place.
6. The data protection training for staff covers data sharing. The policies and procedures have been added to the staff handbook. New staff will be trained during induction and existing staff will have annual refresher training;
7. We must advise the processor that we are the data controller and they are the data processor and outline the processing permitted by following the Data Sharing Procedure for Third Party Processors;
8. Data is routinely shared for the purpose of delivering our course and for reporting and auditing purposes. All external sharing is subject to the processes within the Data Sharing Procedure for Third Party Processors and by following this, we can ensure compliance with data protection requirements;
9. Where a need arises for exceptional sharing of data (one off sharing), the Data Sharing Procedure for Third Party Processors will be followed to ensure compliance with legislative requirements;
10. In order to give full consideration to sharing, we must follow the Data Sharing Procedure for Third Party Processors and complete a DPIA to ensure the checks and balance are completed to ensure that sharing the data is lawful;

11. In order that there is one point of contact to make a complaint, our Privacy Notice only provides the details of our DPO on how to make a complaint. The DPO can make the necessary contact and investigations with the external organisation to resolve the complaint;
12. The Data Sharing Procedure for Third Party Processors gives guidance on how to share data in an emergency situation. It is important to note that not sharing information in an emergency situation could result in serious consequences;
13. We can ensure our policies remain under review by having a schedule of policy and procedure review points;
14. The Data Sharing Procedure for Third Party Processors gives guidance on the review process.
15. We check for any sharing with an individual or organisation based in any country outside of the European Economic Area and ensure that adequate safeguards are in place before sharing commences during the DPIA process;
16. We will undertake a DPIA for all sharing activities with outside organisations. This is not compulsory, however it shows that Essex & Thames Education takes data protection seriously and provides reassurances to individuals.

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.

ICO CONTACTS

Data Protection Officer Sue Rudgley (sue@ete.org.uk)
Senior Information Risk Owner Jo Palmer-Tweed (jo@ete.org.uk)
01268 988580 **Email**: sue@ete.org.uk

For independent advice about data protection, privacy and data sharing issues, you can contact the Information Commissioner's Office (ICO) at:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Tel: 0303 123 1113 (local rate) **or** 01625 545 745 if you prefer to use a national rate number

Alternatively, visit ico.org.uk
https://ico.org.uk/make-a-complaint/

How to Complain

You have a right to make a complaint about the use of your data.

In the first instance, please make your complaint to our DPO, Sue Rudgley, by emailing sue@ete.org.uk.

If you are not satisfied with the response, please contact the ICO on the details above. Our registration number is ZB444055.