THEORISE

Westpoint, 4 Redheughs Rigg, Edinburgh, EH12 9DQ

0131 589 2363

www.theoriseltd.com

Data Protection Procedure

1. Purpose

Theorise Ltd is committed to ensuring that personal information is handled securely, lawfully and in accordance with UK GDPR, the Data Protection Act 2018 and Theorise Ltd policies and procedures.

This procedure provides practical guidance for support staff, employees, contractors and other individuals processing personal data on behalf of Theorise Ltd.

This procedure should be read alongside the Theorise Ltd Data Protection Policy.

---

2. Scope

This procedure applies to all individuals processing personal data on behalf of Theorise Ltd, including:

- Directors
- Employees
- Support Staff
- Contractors
- Temporary Workers
- Volunteers
- Consultants

The procedure applies to all personal information processed in electronic, paper or any other format.

---

3. Responsibilities

All individuals processing personal data on behalf of Theorise Ltd are responsible for:

- Complying with the Data Protection Policy and this procedure
- Maintaining confidentiality
- Protecting personal information from unauthorised access
- Using information only for legitimate business purposes
- Reporting concerns immediately
- Following information security requirements
- Reporting suspected data breaches without delay

Failure to comply with this procedure may result in disciplinary action, removal from assignments, termination of engagement and, where appropriate, legal action.

---

4. Handling Student Information

Support staff may have access to personal information relating to students as part of their support role.

Examples may include:

- Student names
- Contact details
- Course information
- Timetables
- Disability-related information
- Support recommendations
- Reasonable adjustment information
- Support records

Support staff must:

- Access only information required for their role
- Treat all information as confidential

• Store information securely

• Avoid discussing student information in public places

• Ensure information is not visible to unauthorised individuals

• Dispose of information securely when no longer required

Student information must never be accessed out of curiosity or shared with individuals who do not have a legitimate need to know.

---

5. Support Staff Portal Security

Theorise Ltd uses a secure online portal to provide access to Assignment Forms and other operational information.

Access to the portal is restricted to authorised users only.

Users are responsible for:

• Keeping usernames and passwords secure

• Ensuring login credentials are not shared

• Logging out when systems are not in use

• Reporting any suspected unauthorised access immediately

• Maintaining the confidentiality of information accessed through the portal

Support staff must not permit another individual to access the portal using their account.

Portal Address:

https://theoriseltd.opencrm.co.uk/portal/

---

6. Email Security

When using email, individuals must:

• Check recipient details carefully before sending

• Use blind copy (BCC) where appropriate

• Avoid sharing information unnecessarily

• Send only information required for the intended purpose

• Exercise particular caution when sending sensitive personal information

• Report incorrectly sent emails immediately

If information is sent to the wrong recipient:

1. Attempt to recall the email where possible.
2. Contact the recipient requesting deletion.
3. Notify Dany Brunton immediately.
4. Cooperate with any follow-up investigation.

---

7. Device Security

Individuals processing personal data must take reasonable steps to protect devices used for work purposes.

This includes:

• Using secure passwords

• Locking devices when unattended

• Keeping software up to date

• Using anti-virus protection where appropriate

• Avoiding unsecured public computers

• Storing devices securely

• Preventing unauthorised access by family members, friends or other third parties

Lost or stolen devices that may contain personal information must be reported immediately.

---

8. Sharing Information

Personal information must only be shared where there is a legitimate reason to do so.

Information may be shared with:

- Educational institutions
- Funding bodies
- Other authorised support staff
- Regulatory bodies
- Emergency services
- Other organisations where disclosure is legally required

Before sharing information, individuals should consider:

- Whether disclosure is necessary
- Whether disclosure is proportionate
- Whether the recipient has a legitimate need to know
- Whether consent is required

Where uncertainty exists, advice should be sought before information is shared.

---

9. Safeguarding and Welfare Concerns

In certain circumstances, personal information may need to be shared without consent.

This may include situations involving:

- Risk of harm
- Safeguarding concerns
- Serious welfare concerns
- Criminal activity
- Legal obligations

Support staff should follow Theorise Ltd safeguarding procedures and seek advice immediately where concerns arise.

Protecting the safety and welfare of individuals will take precedence where significant risk exists.

10. Subject Access Requests

Individuals have rights under data protection legislation, including the right to request access to personal information held about them.

If a Subject Access Request or similar request is received:

- Do not respond independently
- Forward the request immediately to Dany Brunton
- Preserve any relevant records
- Cooperate with any subsequent enquiries

All requests will be managed centrally by Theorise Ltd.

11. Requests for Correction, Deletion or Restriction

Individuals may request:

- Correction of inaccurate information
- Deletion of information where appropriate
- Restriction of processing
- Objection to processing
- Withdrawal of consent

Support staff must not action such requests independently.

Any such request should be referred immediately to Dany Brunton.

12. Reporting Personal Data Breaches

A personal data breach may include:

- Sending information to the wrong person

- Losing paperwork
- Losing a laptop, tablet or mobile device
- Unauthorised access to information
- Disclosure of confidential information
- Cyber security incidents

Any suspected breach must be reported immediately to:

Dany Brunton
Director
dany@theoriseltd.com

Individuals reporting a breach should provide:

- What happened
- When it occurred
- What information was involved
- Who may have been affected
- Any action already taken

Prompt reporting is essential as certain breaches may require notification to the Information Commissioner's Office within statutory timescales.

---

13. Record Keeping

Support staff should maintain records that are:

- Accurate
- Relevant
- Professional
- Objective
- Securely stored

Only information necessary for the delivery of support services should be recorded.

Records should be retained and disposed of in accordance with Theorise Ltd's Data Retention Policy.

---

14. Complaints

Concerns relating to the handling of personal information should be reported to:

Dany Brunton
Director
dany@theoriseltd.com

Complaints will be managed in accordance with Theorise Ltd's Complaints Policy and Data Protection Policy.

Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO).

---

15. ICO Registration

Theorise Ltd is registered with the Information Commissioner's Office (ICO) as a Data Controller.

ICO Registration Number: ZA430867

---

16. Procedure Review

Item	Details
Procedure Owner	Dany Brunton
Approved By	Director
Version	Version 3.0
Last Reviewed	26/05/2026
Next Review Date	26/05/2027
Review Frequency	Annually

THEORISE

Westpoint, 4 Redheughs Rigg, Edinburgh, EH12 9DQ

0131 589 2363

www.theoriseltd.com