Data Processing Security Measures

Version: 1.0

Date: May 2026

This document sets out Jessanol's standard security measures when processing personal data on behalf of a Client.

It should be read alongside:

- the relevant Data Processing Form;
- the relevant Booking Form, proposal or statement of work;
- the applicable Jessanol terms;
- Jessanol's Privacy Policy;
- Jessanol's Data Protection and Information Security Policy;
- Jessanol's Cyber Security Statement;
- any Client-specific security instructions agreed in writing.

These measures are intended to support appropriate technical and organisational security in line with the nature, scope, context and risk of the processing.

1. Security approach

Jessanol takes a practical and proportionate approach to data processing security.

Jessanol's security approach is informed by recognised good practice, including Cyber Essentials principles, where relevant and proportionate.

Jessanol is preparing for Cyber Essentials certification but does not currently claim to be Cyber Essentials certified unless this is confirmed separately in writing.

Jessanol uses Microsoft Defender to support anti-virus, anti-malware and device security protection on devices used for Jessanol business activity.

2. Relationship with Client-specific security instructions

Jessanol's standard data processing security measures apply unless different or additional Client-specific security instructions are agreed in writing.

Where the Client provides its own security instructions, those instructions will apply in addition to Jessanol's standard measures where relevant, reasonable, lawful and practical for the agreed work.

If there is a conflict between the Client's instructions and Jessanol's standard measures, the parties will agree how to proceed before the relevant processing begins or continues.

Where different security standards apply, Jessanol will normally follow the higher or more protective standard, provided it is lawful, reasonable and practical for the agreed work.

Additional Client-specific security requirements may affect fees, timescales, access arrangements or whether Jessanol can provide the relevant service.

3. Devices and equipment

Jessanol will take reasonable steps to ensure that devices used to access Client personal data are used securely.

This may include:

- keeping devices physically secure and not leaving them unattended in public or shared spaces;
- using strong passwords or passphrases;
- using secure authentication methods where available;
- keeping login details secure and not sharing passwords unnecessarily;
- using device screen locks and automatic locking where available;
- positioning screens to reduce the risk of unauthorised viewing;

- keeping operating systems, software and security tools reasonably up to date;
- using Microsoft Defender for anti-virus, anti-malware and device security protection;
- using firewall protection where available;
- using secure home or office Wi-Fi;
- avoiding public Wi-Fi where possible, or using appropriate safeguards such as VPN or secure tethering;
- securely deleting or destroying personal data before disposing of devices or storage media.

4. Local storage and downloads

Jessanol will avoid downloading Client personal data or confidential information to local devices unless this is necessary for the agreed work.

Where local download or storage is necessary, Jessanol will:

- keep local copies to the minimum needed;
- store files in appropriate secure locations;
- avoid storing Client personal data in unnecessary duplicate locations;
- avoid downloading Client personal data where secure access within the Client's own system is sufficient;
- delete third-party personal data from local systems within six weeks of the end of the booking or project, unless otherwise instructed in writing or where retention is required for legitimate legal, accounting, complaint, audit, quality or compliance purposes.

The Client should tell Jessanol if local storage is not permitted or if specific storage instructions apply.

5. Access control

Jessanol will use Client personal data only for the agreed work and in line with the Client's documented instructions.

Jessanol will:

- access only the systems, files and personal data needed for the agreed work;
- use individual logins where available;
- avoid shared logins where reasonable alternatives are available;
- use the lowest appropriate level of access needed to complete the work;
- notify the Client if access appears excessive, inappropriate or unnecessary;
- remove access or ask the Client to remove access when it is no longer required;
- not knowingly allow unauthorised individuals to access Client personal data.

6. Passwords, logins and authentication

Where Jessanol needs access to Client systems, the Client should provide access securely.

Where possible:

- unique user accounts should be created for Jessanol;
- passwords should not be sent together with login details in the same unprotected message;
- password managers, secure sharing tools or separate communication channels should be used;
- multi-factor authentication should be used where available and appropriate;
- shared passwords should be changed when no longer required.

Jessanol will not knowingly share Client logins with unauthorised individuals.

7. File sharing and document handling

Where Client personal data is shared through platforms such as SharePoint, Google Drive, Dropbox, or similar systems, Jessanol will use the agreed platform and access permissions.

Jessanol will:

- use agreed folders, workspaces or systems where provided;
- avoid unnecessary exports or downloads;
- take reasonable care when sharing files, links or attachments;
- check recipients, permissions and file access before sharing personal data where reasonably possible;
- avoid using personal email or unapproved systems for Client personal data unless agreed;
- avoid sending unnecessary personal data by email where a secure portal, folder or shared workspace is more appropriate.

The Client is responsible for ensuring that any Client-owned folder, platform or workspace is configured securely and that Jessanol is given appropriate access.

8. Email and communications

Where personal data is sent by email or message, Jessanol will take reasonable care to reduce the risk of accidental disclosure.

This may include:

- checking recipient details before sending;
- using secure links or portals where appropriate;
- password-protecting attachments where appropriate;
- sending passwords through a separate channel where used;
- avoiding unnecessary personal data in email content;
- reporting misdirected or suspicious communications promptly where relevant.

9. Sub-processors and associates

Where Jessanol uses authorised sub-processors or associates to support the agreed work, Jessanol will ensure they are subject to appropriate confidentiality, data protection and security obligations.

Jessanol will only give sub-processors or associates access to Client personal data where this is necessary for the agreed work and permitted by the Data Processing Form or written agreement.

Jessanol will require authorised sub-processors or associates to access, use, store, share, return or delete Client personal data only in accordance with the Client's documented instructions and the agreed purpose of the processing.

Jessanol remains responsible to the Client for the data protection compliance of authorised sub-processors used by Jessanol for the agreed processing.

10. Backups, availability and recovery

Jessanol will take reasonable steps to protect the availability of business information and Client work materials.

This may include:

- using reputable cloud-based systems;
- maintaining backup or recovery arrangements where appropriate;
- taking reasonable steps to recover information if a technical issue occurs;
- informing the Client where a significant availability issue affects the agreed work.

Where the Client requires specific backup, retention or recovery arrangements, these should be recorded in the Data Processing Form or agreed in writing.

11. Use of AI tools

Jessanol may use AI tools to support general business activity, planning, drafting, editing, organisation or productivity where this does not involve processing Client third-party personal data.

Jessanol will not use AI tools to process Client third-party personal data unless this is expressly agreed in writing before the processing takes place.

Jessanol will not knowingly enter Client third-party personal data, confidential Client information, commercially sensitive information or unpublished Client materials into public AI tools.

If AI-supported processing is required for reporting, analysis or similar work, the agreed tool, purpose, data types, lawful basis, safeguards and any Client-specific restrictions must be recorded in the Data Processing Form or in a separate written agreement.

Where AI-supported processing is approved, Jessanol will only use tools and arrangements that are considered appropriate for the nature and risk of the processing. This may include a Client-approved tool, an in-house tool, or another tool with suitable contractual, data protection and security safeguards.

Further information is set out in Jessanol's AI Use Policy.

12. Security incidents

Jessanol will notify the Client without undue delay if Jessanol becomes aware of a personal data breach or security incident affecting the Client's personal data processed under the Data Processing Form.

Jessanol will take reasonable steps to:

- contain the incident;
- reduce risk;

- preserve relevant information;
- support the Client's response where proportionate and relevant to the agreed processing;
- review lessons learned and improve practices where needed.

The Client remains responsible for deciding whether a report to the ICO or affected individuals is required where the Client is the Data Controller.

13. Client responsibilities

The Client is responsible for ensuring that any personal data supplied to Jessanol is transmitted, shared and made available securely.

The Client is also responsible for:

- providing clear, lawful and documented data processing instructions;
- ensuring that personal data is accurate, relevant and limited to what is necessary;
- providing appropriate access to Client systems, platforms or files;
- ensuring access permissions are appropriate and limited to what Jessanol needs;
- ensuring Client-owned systems, folders, workspaces and platforms are configured securely;
- removing Jessanol's access when it is no longer required;
- telling Jessanol promptly if instructions, access permissions, security requirements or processing purposes change.

Jessanol is not responsible for personal data that is lost, disclosed, corrupted, accessed or otherwise compromised before Jessanol receives it, or where this arises from the Client's insecure transmission, sharing method, access permissions, systems, instructions or data handling practices.

14. Review

These measures will be reviewed periodically and updated where needed to reflect Jessanol's systems, working practices, legal requirements, recognised security guidance and progress towards Cyber Essentials certification.