CinePath Ltd

Information Security & Data Protection Compliance Framework

Last Updated: November 2025

This internal document defines CinePath Ltd’s policies and operational controls for information security, GDPR compliance, and data protection management across all business systems and services.

1. Information Security Policy

1.1 Purpose

This policy ensures all CinePath information assets are protected against loss, damage, misuse, or unauthorised access.

1.2 Infrastructure

All data and applications are hosted on CinePath's secure on-prem Windows server with Cloudflare as the external gateway. The server resides in a controlled facility with restricted physical access. Automatic backups are stored in an encrypted format in a separate outbuilding.

1.3 Encryption

All network traffic is secured using HTTPS (TLS 1.3). Sensitive files and backups are encrypted using AES■256. Portable drives and removable media must also be encrypted.

1.4 Access Control

Only IT staff, company directors, and the quoting engineer assigned to a project can access associated customer and CAD files. Permissions are role-based, controlled through the Windows access system, and automatically logged.

1.5 Monitoring and Updates

Servers and systems are kept updated with current security patches. Automatic monitoring tools flag unauthorised access attempts. Logs are retained for 12 months.

1.6 Incident Reporting

Any suspected breach or unauthorised activity must be reported immediately to the Data Protection Officer (DPO) – George Pickering.

2. GDPR Data Subject Rights Procedure

2.1 Purpose

This procedure defines how CinePath responds to data subject rights under the UK GDPR, including access, rectification, deletion, restriction, portability, and objection.

2.2 Request Handling Steps

1. Verify identity of the requester (e.g., by email or invoice reference).
2. Log the request in the Data Subject Request Log.
3. Acknowledge receipt within 5 working days.
4. Assess data held and respond within 30 calendar days.
5. Extend by up to 60 days if complex, with notice to the requester.
6. Record outcome and actions taken.

2.3 Escalation

If the request involves multiple data systems or complex deletions, escalate to the DPO for review.

3. Data Breach Response Plan

3.1 Objective

This plan outlines the steps CinePath follows upon detecting or suspecting a data breach.

3.2 Stages

1. **Detection:** System alerts or staff report unusual activity.
2. **Containment:** Disconnect affected systems; stop further data exposure.
3. **Assessment:** Determine type, volume, and sensitivity of compromised data.
4. **Notification:** If risk to individuals exists, notify the ICO within 72 hours and affected users without delay.
5. **Recovery:** Restore from clean backups and patch vulnerabilities.
6. **Review:** Log incident details in the Incident & Breach Log and perform root cause analysis.

4. Data Protection Impact Assessment (DPIA) Summary

Purpose: Evaluate privacy risks associated with processing personal and CAD design data together in Cine3D, ConveyorPro, and related apps.
Risk Management Measures:
- Encryption at rest and in transit.
- Role-based access control limiting exposure.
- Regular review of data retention and deletion.
- Audit logs for access tracking.
- Periodic risk reviews by the DPO.
Review Frequency: Annual or upon major system change.

5. Records of Processing Activities (RoPA)

Data Category	Purpose	Access	Retention
Customer contact info	Quotation, invoicing, communication	Directors, IT staff	7 years
Uploaded CAD / 3D files	Manufacturing and repeat orders	Quoting engineer, IT staff	Until deletion requested
Invoices & payments	Accounting and audit	Finance & Directors	7 years
Website analytics	Performance monitoring	IT staff	30 days

6. Access Control Register

Role	Access Level	Data Areas
Director	Full administrative	All company data, backups, accounts
IT Staff	Technical admin	Server, databases, logs
Quoting Engineer	Limited project-specific	Assigned CAD and quote files only

7. Confidentiality & Non■Disclosure Policy (Staff)

All employees, contractors, and partners must protect CinePath’s data and customer information. No confidential data may be shared, copied, or transmitted outside company systems without written permission. Breach of this policy may result in disciplinary action or legal proceedings.
Staff must sign this policy upon hiring and reaffirm annually.

8. Training Log – Data Protection Awareness

Name	Role	Training Date	Trainer	Notes

9. Incident & Breach Log

Date	Description	Impact Level	Action Taken	Closed By