techrelate
people & technology

COMPLIANCE GUIDE FOR LAW FIRMS

IT Compliance Checklist for Law Firms

A practical review for UK legal practices — work through this in under 15 minutes.

SECTION 1
Data Security & Access Controls

SECTION 2
Email Security

SECTION 3
SRA Compliance

SECTION 4
Business Continuity & DR

SECTION 5
Legal Software & Docs

SECTION 6
Your IT Provider

SECTION 1

Data Security and Access Controls

- [ ] **Client data is stored** in a central, approved system - not on individual desktops or personal drives
- [ ] **Access to client files is restricted** by role - staff can only see what their job requires
- [ ] **All access is auditable** - you can see who accessed what and when
- [ ] **Encrypted storage** is in place for all client data at rest and in transit
- [ ] **Multi-factor authentication** is enabled on all accounts including email, practice management, and client portals
- [ ] **Leavers have access removed** on the day they leave the firm

SECTION 2

Email Security

- [ ] **Advanced email filtering** is in place to catch phishing attempts and malicious attachments
- [ ] Staff have received **training on identifying suspicious emails** in the last 12 months
- [ ] **Payment instruction changes** received by email are verified by phone before action is taken
- [ ] **Shared mailboxes** have appropriate access controls in place

SECTION 3

SRA Compliance

- [ ] Your IT systems support **compliant legal accounting software** with audit trails
- [ ] A **technology risk assessment** has been conducted in the last 12 months
- [ ] **Data retention and deletion policies** are documented and followed
- [ ] **UK GDPR obligations** are reflected in how client data is stored, processed, and deleted
- [ ] IT-related sections of your **professional indemnity questionnaire** are accurately completed
- [ ] You have a documented process for responding to a **data breach or SRA notification** event

SECTION 4

Business Continuity and Disaster Recovery

- [ ] **Daily backups** are in place and include an offsite or cloud copy
- [ ] **Backups are tested regularly** - not just assumed to be working
- [ ] A **written disaster recovery plan** exists and has been rehearsed
- [ ] You know your **recovery time objective** - how long the firm can operate without its systems
- [ ] **Critical systems and contacts are documented** so recovery can begin without key individuals present

SECTION 5

Legal Software and Document Management

- [ ] **Practice management and case management software** is fully supported by your IT provider
- [ ] **Document storage follows a consistent structure** - files are not scattered across desktops and email
- [ ] **Version control** is in place for matter documents
- [ ] **Remote access to firm systems** is secure and meets the same standards as office access
- [ ] **Software licences are current** and systems are kept up to date with security patches

SECTION 6

Your IT Provider

- [ ] Your provider has **experience supporting other UK law firms**
- [ ] They can speak to **SRA compliance requirements** without you explaining them
- [ ] You have a clear **SLA with defined response times** for critical issues
- [ ] There is a **single point of accountability** for your IT - not multiple suppliers pointing at each other
- [ ] Your provider has conducted a **security review of your environment** in the last 12 months

YOUR RESULTS

How many boxes did you tick?

Mostly ticked

Your IT foundations are in good shape. Consider a formal review annually to stay ahead of regulatory changes.

Several gaps

These represent real compliance and operational risk. A conversation with a specialist IT provider is a sensible next step.

Significant gaps

Do not leave these unaddressed. Contact Techrelate for a free consultation.

BOOK A FREE CONSULTATION

SCAN QR TO BOOK

Call 0330 010 0201 **Email** help@techrelate.co.uk