

Document Management Checklist

Proper document management is crucial for regulatory compliance, operational efficiency and protection of sensitive information.

This checklist covers essential documents related to building regulations, equipment maintenance, staff records, and various certifications required to run a dental practice.

Regulatory Compliance

- ☐ Building regulations certificate
- ☐ Health and Safety Executive (HSE) certificate
- ☐ Financial viability forms
- ☐ Information Commissioner's Office (ICO) certificate
- ☐ Statement of purpose

Policies and Procedures

- ☐ Complete set of practice policies
- ☐ COSHH (Control of Substances Hazardous to Health) folder with signs
- ☐ Procedural manuals

Staff Documentation

- ☐ DBS (Disclosure and Barring Service) checks
- ☐ Curriculum Vitae (CV)
- ☐ Professional indemnity certificates
- ☐ Relevant qualifications and certificates
- ☐ References
- ☐ Proof of identification

Insurance and Contracts

- ☐ Waste disposal contracts (e.g., SCRL, PHS, Cannon, Initial)
- ☐ Professional liability insurance policy

Document Management Checklist

Equipment Maintenance and Safety

<input type="checkbox"/> Compressor Pressure Vessel Inspection (PVI) certificate and service records	<input type="checkbox"/> PAT (Portable Appliance Testing) certificates for all relevant equipment
<input type="checkbox"/> Dental chair service records	<input type="checkbox"/> Autoclave PVI certificate and service records
<input type="checkbox"/> Suction pump service records	<input type="checkbox"/> Disinfectant service records
<input type="checkbox"/> Electrical safety certificate	<input type="checkbox"/> X-ray machine service records

Document Storage Tips:

- Regularly review and update documents to ensure compliance with current regulations
- Implement a digital document management system for easy retrieval and backup
- Organise documents by category and date for efficient access
- Use a fireproof, lockable filing cabinet for physical documents

Security Practices for Sensitive Information:

- Use encryption for digital files containing confidential information
- Implement a secure destruction policy for outdated documents
- Limit access to sensitive documents on a need-to-know basis
- Regularly audit document access and security measures
- Train staff on proper handling of sensitive information