Data Protection Toolkit Guide

SMART DENTAL
COMPLIANCE & TRAINING

Ref	Mandatory requirements	Criteria to meet the requirements
1.1	**There is senior ownership of data security and protection within the organization**	
1.1.2	**Who has responsibility for data security and protection and how has this responsibility been formally assigned?**	You must nominate someone within your organization to take overall senior responsibility for data security and protection. This can be an appointed DPO that has been signed an appointment letter and has been given a job description for this role. Needs to be a separation of the SIRO and the DPO. The SIRO (usually practice manager or Board level director) is accountable and owns the data protection risks. The DPO advises, monitors, audits and reports to the practice. They are also the contact person for the ICO and data subjects. Only NHS contract holders or very large private practices are required to have a DPO. Otherwise, the DPO should be renamed to IG lead or Data Protection Lead **DPO Appointment Letter** and **DPO Job Description** available on All-In-One Management software.
1.2	**DPO Appointment Letter and DPO Job Description available on All-In-One Management software.**	
1.2.1	**Does your organisation have up to date policies in place for data protection and for data and cyber security?**	Please ensure that the practice has in place the following documents: • Acceptable Use policy • Record management, retention and destruction policy The policies should be reviewed and approved by the management team or equivalent within the last 12 months. All documents are available on All-In-One Management software.
1.3	**Individuals' rights are respected and supported (GDPR Article 12-22)**	
1.3.1	**What is your organization's Information Commissioner's Office (ICO) registration number?**	Registration with the ICO is a legal requirement for every organization that processes personal information. The ICO number can be found on your annual ICO registration confirmation
1.3.2	**Does your organization have a privacy notice?**	Please attach your Privacy Notice for Staff and Privacy Notice for Patients. These forms can be found on All-In-One Management software.

1.4	**Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and DPA 18 Schedule 1 Part 4)**	
1.4.1	**Does your organization have an up-to-date list of the ways in which it holds and shares different types of personal and sensitive information?**	The list must different ways in which your organization holds personal and sensitive information (e.g., filing cabinet, care planning system, laptop). This list is called an **Information Asset Register** (IAR) and can be found on All-In-One Management software. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, pay slips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organization keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st April 2020.
1.4.4	**Is your organization compliant with the national data opt-out policy?**	99% of practice won't be using patient data outside of provision of treatment. The data opt-out is more for NHS organization that use data for research and statistic purpose. The patient Privacy notice must contain opt out options and staff must be trained to signpost patients to the NHS website if they ever enquire about it. https://digital.nhs.uk/services/national-data-opt-out The **Private Notice** can be found on All-In-One Management software.
1.5	**Personal information is used and shared lawfully**	
1.5.2	**Does your organisation carry out regular data protection spot checks?**	The practice should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. The Data Protection Spot Check Audit is available on All-In-One Management software.

1.6 The use of personal information is subject to data protection by design and by default

1.6.1 Does your organization's data protection policy describe how you keep personal data safe and secure?

The Data protection Policy should describe how your organization keeps personal data as safe as possible.
It should set out, for example: how you might use codes instead of names when sharing data with others; how you might secure or encrypt messages so that only authorized people can read them.
This is called 'data protection by design'.
Your policy should also set out, for example: how you only collect the minimum amount of data that you need, how you limit access to only those who need to know, keep the data for as short a time as possible, and how you let people know what you do with their data, physical security measures. This is called 'data protection by default'.

Data Protection Policy is available on All-In-One Management software.

1.6.2 How does your organization make sure that paper records are safe when taken out of the building?

The practice should edit the Data Protection policy to fit their way of working.

For example:
Paper records containing personal data are occasionally and temporarily removed from the practice. Individuals requesting to remove records from the practice must first obtain approval from {insert position}. The type of record, the purpose, date of removal, expected return date and the name of the person removing the record is logged internally. The person removing the record is responsible for its safe keeping and must ensure the record is not left in an unsecure location (e.g., unlocked car, hotel room etc.).
If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.

1.6.3 Briefly describe the physical controls your buildings have that prevent unauthorized access to personal data.

Lockable windows, lockable doors, lockable drawers, key holder log, alarm, CCTV, key coded door entry for all internal doors, lockable filing cabinets are all physical controls that a practice must have to prevent unauthorized access to personal data.
Refer to data protection policy if physical access controls are mentioned. Practice is responsible for detailing what is actually in place.

1.6.4	**What does your organization have in place to minimize the risks if mobile phones are lost, stolen, hacked or used inappropriately?**	All mobile phones must be protected by PIN, fingerprint and facial scan in case of being lost or stolen. All phones also must have the Android Device Manager app installed to help to keep the device safe and secure along with data inside, also tracking the device associated with Google account, reset the device screen, lock PIN, and erase all data on the phone. This applies to work and personal devices which are used to access personal data controlled by the practice (including work email). Ensure mobile phones are kept UpToDate with the latest software. Jail broken phones are not permitted to be used for work purposes. Not to be connected to the public WIFI. Recommend having a documented practice meeting on this and add to the Data Protection/Security Policy
1.6.5	**Does your organization's data protection policy describe how you identify and minimize risks to personal data when introducing, or changing, a process or starting a new project involving personal data?**	Data Protection Policy should describe the process that your organization has in place to make sure that it systematically identifies and minimizes the data protection risks of any new project or plan that involves processing personal data. Also, you should document whether a DPIA is required at the early stages of a project. Data Protection Policy and DPIA form are available on All-In-One Management software.
1.6.6	**If staff, directors, trustees and volunteers use their own devices (e.g., phones) for work purposes, does your organization have a bring your own device policy and is there evidence of how this policy is enforced?**	If staff, directors, trustees and volunteers use their own devices including laptops, tablets, mobile phones, CDs, USB sticks etc. an upload your Bring Your Own Device Policy is needed. A signatory sheet in required to ensure they have read the policy and a practice meeting has been held. If nobody uses their own devices, then tick and write "Not applicable" in the comments box.

1.7 **Effective data quality controls are in place and records are maintained appropriately**

1.7.2	**If your organization uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed since 1st April 2020? This contract should meet the requirements set out in data protection regulations.**	If your organization uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organization, then the contract(s) or other written confirmation with third parties must include a data processor agreement (this can be separate to the main contract). Usually, the firm will provide the DPA. Ensure it is signed and dated. This includes paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks If you do not use third parties to destroy records or equipment, then tick and write "Not applicable" in the comments box.
1.7.3	**If your organization destroys any records or equipment that hold personal data, how does it make sure that this is done securely?**	If anyone in your organization destroys any records or equipment themselves, such as shredding documents, briefly describe how the organization makes sure that this is done securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box.
1.7.4	**Does your organization have a timetable which sets out how long you retain records for?**	Your organization should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on statutory requirements or other guidance. This is usually located in the record of processing activities

1.8 **There is a clear understanding and management of the identified and significant risks to sensitive information and services**

1.8.2 **What are the top three data and cyber security risks in your organization and how does your organization plan to reduce those risks?**

All organizations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organization.

Example:

- Hacking
- Staff not changing their password often
- Viruses on the computers which may leak information
- Insider threat of data tampering, eaves dropping
- False user IDs
- Lack of accountability
- Fake emails and device protection – especially mobile devices
- Backup failure
- Staff taking a copy of personal data
- Sensitive information sent to the wrong party.

2.2 **Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards**

2.2.1 **Does your organisation have an induction process that covers data security and protection, and cyber security?**

All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.
This should be covered in covered in your Induction Policy and Procedure, Data Security and Data Retention Policy and Procedure.

All documents are available on All-In-One Management software.

2.2.2 **Do all employment contracts, and volunteer agreements, contain data security requirements?**

All employment contracts should have the data security requirements in them or the employed team members have signed either the Staff Confidentiality Agreement.
The practice must check if there is clause in the self-employed contract that means they must follow practice policies (state that they should seek legal advice due to the workers status issue). Or ensure there is a confidentiality clause in the contract.
This document is available in the GDPR Folder on All-In-One Management software.

3.1 **There has been an assessment of data security and protection training needs across the organisation**

3.1.1 **Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st April 2020?**

A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organization.
Training needs analysis should state the whole staff should undertake NHS level 1 data security protection training (or similar) and management, DPOs and SIROs need to have completed advanced data protection training relevant to their role

All staff members, directors, trustees and volunteers must have an annual Data Protection and Security Training Needs Analysis completed annually.

3.2 **Staff pass the data security and protection mandatory test**

3.2.1 **Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st April 2020?**

All people in your organization with access to personal data must complete appropriate data security and protection, and cyber security, training every year.

GDPR CPD training is available for all staff members on All-In-One Management software or e-LfH Hub

3.4 **Leaders and board members receive suitable data protection and security training**

3.4.1 **Have the people with responsibility for data security and protection received training suitable for their role?**

The practice training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).

4.1 **The organization maintains a current record of staff and their roles**

4.1.1 **Does your organization have an up-to-date record of staff, and volunteers if you have them, and their roles?**

The practice must have a list of all staff, and volunteers and their current role.
This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.
The practice manager should maintain an organization chart in the Annual Management Review and is update it annually.

4.1.2	**Does your organization know who has access to personal and confidential data through its IT system(s)?**	All staff must have a unique login to systems that hold patient data. The same goes for HR date systems also. A list of persons with access and permissions is contained in the practice management software. The IG Lead should carry out a risk assessment annually. If your organization does not use any IT systems, then tick and write "Not applicable" in the comments box.
4.2	**Organization assures good management and maintenance of identity and access control for its networks and information systems**	
4.2.5	**Does your organization have a reliable way of removing or amending people's access to IT systems when they leave or change roles?**	When people change roles or leave the practice, there needs to be a reliable way to amend or remove their access to the IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. You can use the Employee Leavers Checklist available on All-In-One Management software.
4.3	**All staff understand that their activities on IT systems will be monitored and recorded for security purposes**	
4.3.1	**Have all the administrators of your organization's IT system(s) signed an agreement to hold them accountable to higher standards?**	The signed agreement can be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organization does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.
4.5	**You ensure your passwords are suitable for the information you are protecting**	
4.5.4	**How does your organization make sure that staff, directors, trustees and volunteers use good password practice?**	Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. The passwords should include a mixture of letters and numbers which makes them hard to guess. Password policy is included in Data Security policy. Have a documented practice meeting. Encourage staff to check if their password is on the dark web https://haveibeenpwned.com/ https://howsecureismypassword.net/ tests the password strength. Should be plus 1000 years

5.1	**Process reviews are held at least once per year where data security is put at risk and following data security incidents**	
5.1.1	**If your organization has had a data breach or a near miss in the last year, has the organization reviewed the process that may have allowed the breach to occur?**	If the practice has had a data breach or a near miss in the last 12 months, has this been reviewed annually? This includes unauthorized devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. This needs to be minute meeting or otherwise documented discussion between DPO and SIRO. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.
6.1	**A confidential system for reporting data security and protection breaches and near misses is in place and actively used**	
6.1.1	**Does your organization have a system in place to report data breaches?**	All staff members are responsible for noticing and reporting data breaches in the organization. This needs to be documented. E.g., inform the Practice Manager, DPO immediately, decide within 72 hours whether it needs to be reported to the ICO (data subjects too for high-risk incidents) NHS practices can report breaches using the DSP Toolkit incident reporting tool
6.1.4	**If your organization has had a data breach, were the management team notified, and did they approve the actions planned to minimize the risk of a recurrence?**	In the event of a data breach the management team of your organization, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. The discussions and actions taken to minimize the risk of a recurrence needs to be minute meeting or otherwise documented discussion between DPO and SIRO. If no breaches in the last 12 months, then please tick and write "Not applicable" in the comments box
6.1.5	**If your organization has had a data breach, were all individuals who were affected informed?**	If the practice has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g., damage to reputation, financial loss, unfair discrimination, or other significant loss - you must be honest and inform the individual(s) affected as soon as possible. If your organization has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

6.2 **All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway**

6.2.3 **Do all the computers and other devices used across your organization have antivirus/anti-malware software which is kept up to date?**

All servers, desktop computers, laptop computers, and tablets must have malware software. You may need to ask your IT supplier to assist with answering this question.
If your organization does not use any computers or other devices, then tick and write "Not applicable" in the comments box.

6.3 **Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses**

6.3.1 **If you have had a data security incident, was it caused by a known vulnerability?**

If the practice recorded a data security incident over the reporting period (a year), please provide details of incidents.

If no incidents have occurred mark None.

6.3.2 **Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?**

All staff members should be aware that use of public Wi-Fi (e.g., Wi-Fi freely available at cafes and train stations etc.) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorized access of personal data.
Written evidence, could be a practice meeting, memo, policy sign off

If nobody uses mobile devices for work purposes out of your building/offices, then tick and write "Not applicable" in the comments box.

7.1 **Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services**

7.1.2 **Does your organization have a business continuity plan that covers data and cyber security?**

Business Continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g., through fire), emergency contact numbers, IT providers, Insurance companies.
Business Continuity Plan is available on All-In-One Management software.

7.2 **There is an effective test of the continuity plan and disaster recovery plan for data security incidents**

7.2.1 **How does your organization test the data and cyber security aspects of its business continuity plan?**

Describe how your organization tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be since 1st April 2020.

- Documented check that the DPO and SIRO have reviewed and tested this.
- Check anti-virus is working
- Staff have done training
- Contact numbers work
- Insurance policies are active

7.3 **You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions**

7.3.1 **How does your organization make sure that there are working backups of all important data and information?**

It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Recommend that practices should engage their IT support to check the health of the most recent back up.

7.3.2 **All emergency contacts are kept securely, in hardcopy and are up-to-date.**

Emergency Contacts details should be available in the Business Continuity Plan.
Provide location of BCP (hard copy)

7.3.3 **Are backups routinely tested to make sure that data and information can be restored?**

The organization's backups should be tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example).
You may need to ask your IT supplier to assist with answering this question.

If your organization does not use any computers or IT systems, then tick and write "Not applicable" in the comments box.

8.1 **All software and hardware have been surveyed to understand if it is supported and up to date**

8.1.4 **Are all the IT systems and the software used in your organization still supported by the manufacturer or the risks are understood and managed?**

All the Systems and software used in the practice should be supported by the manufacturer. You may need to ask your IT supplier to assist with answering this question.

If your organization does not use any IT systems or software, then tick and write "Not applicable" in the comments box

8.2 **Unsupported software and hardware are categorized and documented, and data security risks are identified and managed**

8.2.1 **If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarizes the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organization is taking to minimize the risk.**

This document should indicate that your management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. Reasons for using the unsupported software is that it is required to view legacy records. It is protected by the IT firewall; the software is on a standalone computer not connected network. Or is an uncommon piece of software (e.g., historical imaging software) therefore unlikely to be targeted by a cyber-attack.

NB Operating software (e.g., Windows) and browsers (Chrome, Edge) need to be kept updated as they are targeted.

8.3 **Supported systems are kept up-to-date with the latest security patches**

8.3.2 **How does your organization make sure that the latest software updates are downloaded and installed?**

The organization's IT system(s) and devices must have the latest software and application updates installed.
Most software can be set to apply automatic updates when they become available from the manufacturer.
This can be done weekly and the manufacturer can send emails to the practice when the updates are done.
You may need to ask your IT supplier to assist with answering this question.

If your organization does not use any IT systems, devices or software, write "Not applicable" in the text box.

9.1 **All networking components have had their default passwords changed**

9.1.1 **Does your organization make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?**

Networking components include routers, switches, hubs and firewalls at all of your organization's locations.
Your organization may just have a Wi-Fi router. Staff are advised that the router admin password is changed.
You may need to ask your IT supplier to assist with answering this question.

If your organization does not have a network or internet access, then tick and write "Not applicable" in the comments box.

9.6 **You securely configure the network and information systems that support the delivery of essential services**

9.6.2 **Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?**

Staff can use Bitlocker for USB pens https://www.dummies.com/computers/operating-systems/windows-10/how-to-use-bitlocker-for-encryption-on-removable-drives/
IT supplier can help with Laptop drive encryption.
Use android and Apple encryption by forcing a pin code on the device.
If your organization does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box.

10.1 **The organisation can name its suppliers, the products and services they deliver and the contract durations**

10.1.2 **Does your organization have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?**

Your organization should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, referral platforms, HR and payroll services, showing the system or services provided.

List of suppliers who process Personal information is available on All-In-One Management software.

If you have no such suppliers, then 'tick' and write “Not applicable” in the comments box.

10.2 **Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance**

10.2.1 **Do your organisation’s IT system suppliers have cyber security certification?**

The key IT system suppliers to check are:

- Practice Management System
- HR systems
- Compliance Systems
- Referral platforms
- IT support
- Digital scanners
- Payroll systems

If they don’t’ have the certification then an action plan needs to be created to ensure they achieve at least cyber essentials within a set period.
If your organization does not use any IT systems, then tick and write “Not applicable” in the comments box.