lichfield dental care

Data Protection Policy

1. **General**

The practice collects, holds, processes and shares personal data in accordance with the provisions of the General Data Protection Regulation and the Data Protection Act 2018. We have carried out and will review as appropriate, a Data Audit.

This Policy applies to personal data in the following categories:

- Patients' Records, both current and past
- Employees' data
- Contractors' data - including dental registrants
- CCTV footage

2. **Data Protection Principles**

We shall ensure that Personal Data, including Special Data (health) will be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes only
- Adequate, relevant and necessary for the purpose
- Accurate and updated
- Kept for no longer than is necessary
- Processed in a secure manner and protected against loss, destruction or damage

3. **Lawful Basis**

Data will be held and processed under the following Lawful Basis:

- Patient Data and health records: for the Legitimate Interests of the practice in providing health care and treatment
- Employment records: as a Legal Obligation for the provision of Employment Terms and conditions and supply of data to HM Revenue and Customs and other statutory functions such as pensions and benefits
- Contractor Data: for the fulfilment of contracts
- CCTV Data: for the detection and prevention of crime

We will additionally secure the specific consent of patients for the provision of electronic communication under the Privacy and Electronic Communication Regulations 2011

4. **Data Subjects' Rights**

We will ensure that the rights of Data Subjects are respected and maintained by:

- The issue and promotion of a Privacy Notice detailing data processed, its origin and any disclosures, the Lawful Bases for processing, and the rights of Data Subjects
- The maintenance of a Subject Access process and the appointment of Lynsey Mason as Data Protection Officer to oversee that process and to advise on compliance
- A legitimate interest assessment ensuring individuals' rights are balanced with the legitimate needs of the practice.
- A Data Retention schedule

- An Information Security policy
- A Data Breach Policy
- Contractual assurance of adequate safeguards if data is processed outside the European Union

5. Subject Access Requests

All data subjects may submit a request to be informed of the data we hold about them, its lawful basis and from whom it is/was obtained and to whom it may be disclosed. We will provide this information without charge and as soon as is reasonably possible and in any event within one month of a valid request being received. Access requests should be addressed (or forwarded without delay) to Lynsey Mason.

6. Training and Compliance

We will ensure that all staff are aware of their duty of strict confidentiality regarding personal data, both professional and under the Data Protection law. We will provide training and assure compliance and will review and refresh training on a regular basis.

It is a condition of continuing employment that all staff are aware of, sign their acceptance of, and comply with, their obligations under this Policy. Any queries or concerns must be immediately addressed to Lynsey Mason. A breach of this Policy may amount to misconduct and result in disciplinary action. Serious or persistent breaches may result in dismissal.

7. Security of Data

The practice will publish and maintain an Information Security policy to assure against any loss, damage, unlawful disclosure or non-compliant erasure of data. All staff will be trained and advised of their obligations under this Policy.

lichfield dental care

Privacy Notice

We are a Data Controller under the terms of the Data Protection Act 2018 and the requirements of the EU General Data Protection Regulation.

This **Privacy Notice** explains what Personal Data the practice holds, why we hold and process it, who we might share it with, and your rights and freedoms under the Law.

Types of Personal Data

The practice holds personal data in the following categories:

1. Patient clinical and health data and correspondence.
2. Staff employment data.
3. Contractors' data.

Why we process Personal Data (what is the "purpose")

"Process" means we obtain, store, update and archive data.

1. Patient data is held for the purpose of providing patients with appropriate, high quality, safe and effective dental care and treatment.
2. Staff employment data is held in accordance with Employment, Taxation and Pensions law.
3. Contractors' data is held for the purpose of managing their contracts.

What is the Lawful Basis for processing Personal Data?

The Law says we must tell you this:

1. We hold patients' data because it is in our **Legitimate Interest** to do so. Without holding the data we cannot work effectively. Also, we must hold data on NHS care and treatment as it is a **Public Task** required by law.
2. We hold staff employment data because it is a **Legal Obligation** for us to do so.
3. We hold contractors' data because it is needed to **fulfil a contract** with us.

Who might we share your data with?

We can only share data if it is done securely and it is necessary to do so.

1. Patient data may be shared with other healthcare professionals who need to be involved in your care (for example if we refer you to a specialist or need laboratory work undertaken). Patient data may also be stored for back-up purposes with our computer software suppliers.
2. Employment data will be shared with government agencies such as HMRC.

lichfield dental care

Your Rights

You have the right to:

1. Be informed about the personal data we hold and why we hold it.
2. Access a copy of your data that we hold by contacting us directly: we will acknowledge your request and supply a response within one month or sooner.
3. Check the information we hold about you is correct and to make corrections if not
4. Have your data erased in certain circumstances.
5. Transfer your data to someone else if you tell us to do so and it is safe and legal to do so.
6. Tell us not to actively process or update your data in certain circumstances.

How long is the Personal Data stored for?

1. We will store patient data for as long as we are providing care, treatment or recalling patients for further care. We will archive (that is, store it without further action) for as long as is required for legal purposes as recommended by the NHS or other trusted experts recommend.
2. We must store employment data for six years after an employee has left.
3. We must store contractors' data for seven years after the contract is ended.

What if you are not happy or wish to raise a concern about our data processing?

You can complain in the first instance to [us] [our Data protection Officer, who is *Lynsey Mason email:*practicemanager@getasmile.co.uk *or by calling 01543 264557 and* we will do our best to resolve the matter. If this fails, you can complain to the Information Commissioner at www.ico.org.uk/concerns or by calling 0303 123 1113.

lichfield dental care

Data Protection Breach Notification Form

ICO Registration Number : Z883456X

Mandatory details (*)

Section 1: Notification of Breach			
1.*	Date and time incident was discovered		Act as soon as reasonably practical: individual reporting incident to complete
2.*	Date incident occurred if different to above		
3.	Location of incident		e.g. on business premises, at home, in car, etc.
4.	Name of individual reporting incident		
5.	Contact details of individual reporting incident (e-mail & phone)		
6.*	Description of incident and details of lost data		How did the breach occur? Did the data refer to identifiable living individuals?
7.*	Number of data subjects affected if known or approximate		
8.	Brief description of any immediate action taken when discovered		e.g. incorrectly addressed e-mail deleted by recipients; data subject advised, etc.

Section 2: Severity Assessment			
9.	Details of IT system/s, equipment, devices and/or data records involved in the breach		Give as much detail as possible
10.	What information was lost?		Brief description of the category e.g. clinical records, employment data
11.*	What is the nature of the information?		e.g. health data, personal records, financial details
12.	How much data has been lost?		Estimate file sizes, number of records etc. Were entire systems affected?
13.*	Is the information retrievable or replaceable?		Was the data effectively backed up? When? Has it been checked? How old is the back-up?
14.	How many data subjects		E.g. number of patients,

	are involved?		employees affected?
15.	Was the data encrypted?		Details of encryption system used if available
16.*	Is the data sensitive?(GDPR: special under Article 9)		Does data concern health, race or ethnicity, politics or religion
17.*	Do the data subjects include children (<18 years) or vulnerable adults		If so specify approximate numbers or percentages
18.	Does the data include information that could facilitate identity theft?		Does the data include banking details, NI numbers, photocopies of passports or similar
19.*	Does data include information which could cause significant distress or damage?		e.g. details of performance, disciplinary action, or personal lifestyle
20.	Does the information contain security data which might compromise the safety of individuals?		e.g. Access codes, confidential address data, etc.

Section 2: Action Taken (for completion by Data Protection Officer)			
21.*	Name of Data Protection Officer		Include contact details if reporting to ICO
22.	Date and time of receipt of report		
23.	Immediate action taken		e.g. Back-up checked or requested, passwords changed, IT company contacted
24.	Police notified?	- Y/N - Crime number - Badge number/name of Officer/contact - Force name or contact details	e.g. theft of laptop, computer or device, malicious cyber-activity or other criminal action
25.	ICO Notified?	- Y/N - Date and time of notification	Include name of organisation and registration No. if known plus all mandatory details (*), and any previous incidents
26.	Other external stakeholders or regulators notified		e.g. CQC or similar regulator legal advice sought; IT or technical advice sought
27.	Other actions taken by Principals/Data Protection Officer		

lichfield dental care

28.*	Have affected Data Subjects been notified of loss or theft?	Y/N	Give reason(s) for action taken or proposed
29.	Further Action recommended		

Signature of person reporting breach: _____

Print Name: _____

Date: _____

Signature of Data Protection Officer: _____

Print Name: _____

Date: _____

Note: if the data breach includes information which:

- could cause significant distress or damage to individuals, or
- could compromise the safety of individuals, especially children or vulnerable adults, or
- is of a volume or nature which may cause serious reputational damage

Then consideration should be given to notifying the ICO and also taking advice from expert external sources.

Reports to the Information Commissioner should be made within 72 hours to casework@ico.org.uk with 'DPA Breach Notification form' in the subject field. Further information can be found at: www.ico.org.uk/ - search 'Personal data breaches'.

This record should be kept even if no adverse consequences are anticipated or notifications are required.

lichfield dental care

Policy Relating to Accidental Disclosure of Confidential Information

At Lichfield Dental Care we are aware of Article 5 (1) (f) of the General Data Protection Regulation which states that personal data shall be:

"...protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

If a Data Breach occurs, we would take the following steps:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

Containment and Recovery

As soon as a breach of confidentiality is discovered, we would assign a person to be responsible for ensuring that the breach is documented using our Data Breach template, and contained. We would establish who needs to be aware of the breach and how they can help in containing it. This may involve shutting down computer systems or establishing new access codes, finding new safe storage for record cards, or changing locks on doors.

We would act to recover any lost or corrupted data as soon as possible <using back up tapes/restoring lost or damaged data from off-site back up>.

Assessment of Ongoing Risk

We would access the type of data involved and its level of sensitivity. We would also assess how much data was involved and the number of people affected.

We would endeavour to find out what has happened to the data and if stolen, whether it could be used harmfully. We would assess whether the data could lead to physical risk, significant distress or damage for the people involved. We would also assess whether the information could lead to identity fraud or financial loss.

Dependent on the type of data we would also assess the damage to the reputation of the practice.

Notification of Breach

We would decide who needed to be informed of the breach. This would be based on who was involved and the type of information. We would make sure that we were meeting our security obligations with regard to the principles set out in Article 5 of the GDPR. We would also make sure we have a clear purpose as to our reasons for notifying affected individuals.

If we felt it was appropriate in that:

- The volume or nature of data loss was significant;
- The data related to children or vulnerable persons;
- The data was likely to cause significant distress or damage to individuals;
- The data was likely to incur significant reputational damage to the practice

- Then we would consider making notification as appropriate to:

- The Information Commissioner (within 72 hours of discovery)
- Healthcare regulator
- NHS authorities

We would discuss with our defence organisation how we should inform the people affected by the breach and what we should say to them. We would make sure we had a contact point in the practice for anybody who had queries to be able to contact.

If it was felt necessary we would inform the ICO. For guidance on whether to inform them we would go to www.ico.org.uk

Evaluation and Response

We would investigate the cause of the breach and how we responded to it. We would review all aspects and update our policies and procedures in light of what we found.

We would ensure that our Data Breach template was completed for every breach, no matter how apparently slight or insignificant, so that we could learn from every issue and take appropriate corrective action for the future.

We would look for any weak points in our system and work to improve them. This may involve further training of staff, assignation of responsibilities and ongoing monitoring.

lichfield dental care

Data Retention Schedule

Under the Data Protection Act 2018 and the General Data Protection Regulation

Data Category	Commencement of Retention Period	Minimum Recommended Retention Period	Maximum Duration of Archived Retention	Notes
Patient clinical data – adults (unless listed below)	Discharge or last entry in record	○ 11 years	○ 30 years	Maximum retention period as advised in IGA RMCoP 2016*
Patient clinical data – children (unless listed below)	Discharge or last entry in record	At age 25 (or age 26 if last entry at age 17) or 11 years whichever is the later	○ 30 years	As above & British Medical Association recommendation for General Practice records
Patient clinical data for those with long-term unresponsive clinical conditions	Date of last entry in record		○ 30 years	IGA RMCoP
Clinical audit records	Date of audit		○ 5 years	Where identification of individual patients is possible (IGA RMCoP
Staff records, Occupational Health records	Date of leaving		○ 6 years	IGA RMCoP
Staff records: timesheets	Date of creation		○ 2 years	IGA RMCoP
Contracts for services	Date of cessation of contract		○ 6 years	e.g. self-employed staff or maintenance contracts (Statute of Limitations)
Financial records	Date of completion of record		○ 6 years	HMRC recommendation: look-back period
Data Category	**Commencement of Retention Period**	**Minimum Recommended Retention Period**	**Maximum Duration of Archived Retention**	**Notes**
Subject Access Requests	Date of supply of information		○ 3 years	IGA RMCoP
CCTV records	Date of recording		○ 3 months	Duration of time necessary e.g. to report and investigate crime
Software licences	Date of inception		○ Lifetime of software	Data must be supplied to data controller and erased when contract expires
Significant incident log	Date of incident		○ Major – 20 years ○ Minor – 10 years	IGA RMCoP Non-clinical – 12 years advised

67 Shortbutts Lane, Lichfield, Staffs, WS14 9BU Tel: 01543 264557
www.getasmile.co.uk

lichfield dental care

*Medical Records Code of Practice (2016): Information Governance Alliance/DHSC/NHS Digital

Signature of Data Protection Officer/Data Controller: _____

Print Name: _____

Review Date: _____

Signature of Director _____

Print Name: _____

Review Date: _____

lichfield dental care

Cookie Policy

What are Cookies?

Your Privacy online is important to us. As is usual with the majority of websites, this site uses Cookies, which are small text files that are automatically downloaded to your computer in order to improve your browsing experience. In this Policy, we describe what information they collect, how we use it and why we sometimes need to store these Cookies. We will also share with you how to prevent Cookies of different kinds being stored, but please note that doing this may interfere with this website and its operation.

- For more information on Cookies, go to: www.AboutCookies.org

How we use Cookies

We use Cookies for a number of reasons which are set out in the sections below. Unfortunately, there are no standard options for disabling all Cookies completely without damaging the features they add to a website. You can choose your options at the end of this Policy.

Disabling Cookies

You can prevent the setting of Cookies by going to your web browser settings (go to the Help page in the browser menu). Depending on your browser type, you may be able to choose which types of Cookies you disable.

The information regarding the Cookies we set is available on our website.

lichfield dental care

Information Security Policy

1. General

Lichfield Dental Care takes seriously its obligations, both in law and against professional standards, to maintain a high standard of security around all data which it holds and processes, and particularly personal and special (health) data (as defined in the Data Protection Act 2018 and the General Data Protection Regulation (EU)).

- Name Lynsey Mason
  Email practicemanager@getasmile.co.uk Phone: 01543 264557
  is designated as the Information Security Officer for the practice and;

- Name Bean IT Ltd
  Email info@beanit.co.uk phone: 0182768613
  is designated as the Technical Support Advisor

All issues related to Information Security shall be reported to the information Security Officer without delay.

2. Access to Personal Data – Digital

All employees and contractors with access to personal data held by the practice must adhere to the following requirements:

(a) A personal log-in and secure password (as approved by the practice) must be used on each occasion that digital data is accessed
(b) Under no circumstances shall the password be divulged to any other person nor shall it be written down or stored on any device
(c) No personal data shall be accessed or processed in any way other than for the purposes it was obtained as set out in the practice's Privacy Statement
(d) All computers and other devices must be locked to a secure screen-saver mode when not in active use
(e) Computers and other devices shall not be used so as to permit any unauthorised viewing or processing of personal data
(f) No personal data shall be copied, downloaded or transmitted to any device or storage medium other than those authorised by the Information Security Officer
(g) No applications, programs or other functionality shall be downloaded or placed on any practice computer or device other than those authorised by the Information Security Officer
(h) Extreme care shall be taken when opening any file attachment originating outside the practice and in any case of doubt the Information Security Officer shall be advised before so doing
(i) No information about practice systems, log-in or other technical details may be provided to any person without the authority of the Information Security Officer
(j) No device or computer may be connected to the practice internet router or any server without the prior consent of the Information Security Officer

3. Environmental Security

All employees and contractors of the practice must adhere to the following requirements to ensure that the practice maintains security around personal data:

(a) All patient records, radiographs, correspondence and other items which can identify an individual person shall be kept in a secure location which is locked or suitably protected from unauthorised access as approved by the Information Security Officer
(b) The practice premises must be securely locked against unauthorised entry when closed and any alarms must be set and checked by those authorised to do so
(c) All desks and work surfaces shall be cleared of material which could identify an individual person when not in use including telephone and other notes
(d) Incoming telephone recording messages shall be cleared and deleted from the system once they have been actioned
(e) No material which can identify an individual person shall be left in such a position that it can be viewed by unauthorised people
(f) CCTV recordings which may depict individual persons shall be deleted from the system at three monthly intervals

4. Internet and External Security

The practice will apply suitable security programs to all systems so as to prevent the introduction of malware or allow unauthorised access, including but not limited to firewalls and anti-virus software as approved by the Information Security Officer and/or the Technical Support Adviser. All software, including the above, will be regularly updated as required.

Penetration testing of the computer, security and telephone systems may take place at intervals and may not be advised in advance to staff and contractors who should therefore maintain vigilance at all times

5. Data Back-up

All personal data will be backed-up on a daily basis using personnel, processes and devices as approved by the Information Security Officer. Back-ups will be audited and confirmed as effective on a regular basis.

6. Off-site Data and Security

Where the information Security Officer has authorised that any personal or other data may be taken or transferred off-site (outside the practice location):

(a) All such authorisations shall be written and a record kept
(b) Authorised data and devices shall be used only for the purposes and period authorised
(c) The requirements in Clause 2 of this Policy will apply to all such instances
(d) Any loss or damage to devices or data must be *immediately* reported to the Information Security Officer and a Data Breach notification template prepared
(e) Devices and data must be secured and out of sight to unauthorised persons whilst in transit and shall be kept in a locked environment when not in use

lichfield dental care

7. Financial Data

When digital payments are taken from patients or other parties at the practice, all staff or contractors will:

(a) Ensure that the requirements of the EFTPOS (Electronic Funds Transfer – Point of Sale) device/s and systems supplier are followed at all times
(b) Ensure that PCI (Payment Card Industry) best practice guidance is followed
(c) Take all precautions against fraud or misuse of payment cards
(d) In particular ensure that no payment card details are written down

8. Internet and E-mail Use

All staff and contractors will follow the practice rules for use of the internet and e-mails and adhere in particular to any requirements or restrictions on:

(a) Personal internet browsing
(b) Sending or receiving personal e-mails
(c) The encryption of authorised practice e-mails containing patient or other personal data

9. Destruction of Data

Data shall only be destroyed with the explicit written consent of the Information Security Officer and using methodology which is secure and approved. Paper data such as notes, jotters which contain personal information will be shredded on the premises or using an authorised contractor.

Devices to be de-commissioned will have all data securely removed from them using an authorised contractor: it is acknowledged that routine formatting or factory re-setting will not suffice.

10. Other

All staff and contractors shall at all times take utmost care and diligence in protecting all data, including personal and health-related data, within the practice.

The practice undertakes to regularly train and update staff on the processing of data held, whether digital or otherwise in order to assure the competence of all users and maintain awareness of data protection and information security.

All and any concerns about the security of data held by the practice, however apparently slight, shall be brought at once to the attention of the Information Security Officer and it shall be the policy of the practice that any such information shall be positively and constructively received to encourage prompt and vigilant awareness of the importance.

Any breach of the terms of this policy may lead to disciplinary action against staff or contractors and repeated or serious breaches may be regarded as serious misconduct resulting in termination of employment or engagement.

lichfield dental care

Review / Change History

Notes	Date
Policy created	17/05/2018

67 Shortbutts Lane, Lichfield, Staffs, WS14 9BU Tel: 01543 264557
www.getasmile.co.uk