01384 292666

**Wall Heath Dental Practice Data Protection Handbook**
**General Policies**

These policies and procedures have been approved by the undersigned, and they will be reviewed on at least an annual basis and in particular in the event of an incident

This manual is to be read in conjunction with the Wall Heath Dental Practice Data Protection Handbook - Policies and Risk Assessments Specific to Wall Heath Dental Practice.

| | |
|---|---|
| **Name** | **(Joanne Thompson)** |
| **Version** | **19** |
| **Date approved** | **1/2/2025** |
| **Review date** | **01/02/2026** |

## Contents

## Access Control Procedures

**Introduction**

Technical access controls are built into information systems by practice IT system suppliers. To ensure confidential information is protected, this functionality must be supported by operational and managerial controls put in place by the practice.

**Purpose**

The Access Control Procedures set out how the Wall Heath Dental Practice will allocate, manage and remove access rights to computer systems holding patient information so that only authorised personnel have access to use and share information held within those systems; and they aim to ensure that access rights are used appropriately by practice staff.

**Scope**

These procedures relate to access controls for computer-based information systems managed by the dental practice to store patient identifiable data. They therefore cover the allocation, management and removal of user accounts and the guidelines provided to dental practice staff to ensure they use the practice-managed system appropriately.

**Summary of technical access controls**

The R4 practice computer system has the following technical controls in place:

- User accounts which restrict access to different areas of R4;
- Passwords required to log on to system;
- Passwords are not displayed on the screen;
- An audit trail which records all actions.

**Responsibility for user access management**

The practice has assigned responsibility for managing user access rights to the system to Joanne Thompson (Partner), who has administrator rights allowing access to sensitive areas (for example, passwords). The unnecessary allocation and use of administrator rights is often found to be a major contributing factor to the vulnerability of systems that have been breached, therefore allocation of administrator rights to other staff can only be authorised by Joanne Thompson.

**General**

Each user is identified by a unique user ID so that users can be linked to and made responsible for their actions. The use of group IDs is only permitted where they are suitable for the work carried out (e.g. training accounts logging on to Windows). During their induction to the system each user is given a copy of guidelines for staff on use of the system and their user login details, and is required to sign to indicate that they understand the conditions of access. A record is kept of all users given access to the system.

**New permanent staff**

When a new employee/contractor joins the practice Joanne Thompson arranges access to the system.

**Locum staff**

Temporary access is granted on a need to use basis. Such logons are granted by Joanne Thompson (Partner) and are recorded and reported in the usual way. Temporary logons are identified by a specific login (T***) and are deleted immediately when no longer required.

**Change of user requirements**

Changes to requirements will normally relate to an alteration to the level of access used or suspension of an account, e.g. if the user is on long-term leave, a locum who returns to the practice from time to time. Requests are made to Joanne Thompson and a record is kept of all changes.

**Password management**

The practice R4 system has no password protection features but staff are asked to:

- Change their password after the first logon;
- Select complex passwords using a combination of upper and lower case letters, numbers and symbols. Passwords should be at least 8 characters long.
- Change their passwords periodically and at least every 6 months;
- Not reuse the same password;
- Change their password immediately if they suspect it has been compromised.

The frequency that passwords should be changed has been increased to 6 months. This is as a result of staff problems remembering passwords and as a result writing them down. We feel that it is more secure to change less frequently and encourage committing passwords to memory. Passwords can be written down as long as they are kept in a secure locked location away from the computers. Currently the only option on the premises is in a staff member's locker.

Passwords will be changed immediately should there be an incident or whenever a member of staff leaves.

**Forgotten password**

Where a user has forgotten his/her password, a replacement should be requested from Joanne Thompson, who issues a temporary, single use, password. The user should change their password to one they are more likely to remember after the first logon.

**Removal of users**

As soon as an individual leaves the practice, all his/her system logons are revoked. As part of the employee termination process Joanne Thompson will revoke their access. This also applies to self-employed contractors such as associates.

**Review of access rights**

Joanne Thompson reviews all access rights on a regular basis, but in any event at least once a year. The review is designed to positively confirm all system users. Any lapsed or unwanted logons, which are identified, are disabled immediately and deleted unless positively reconfirmed.

**Monitoring compliance with access rights**

The management of access rights is subject to regular compliance checks to ensure that this procedure is being followed and that practice staff are complying with their duty to use their access rights in an appropriate manner. Areas considered in the compliance check include whether:

- Only staff regularly working in the practice are registered as active users on the system;
- Allocation of administrator rights is restricted;
- Access rights are regularly reviewed;
- There is any evidence of staff sharing their access rights;
- Staff are appropriately logging out of the practice system.

**Approval and review**

These procedures have been approved, and they will be reviewed on at least an annual basis and will take into account changes made to the technical access controls in systems by dental practice system suppliers.

## Accidental Disclosure of Confidential Information

At Wall Heath Dental Practice 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 breach occurs we would take the following steps:**
1. Containment and recovery;
2. Assessment of on-going 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 the data as soon as possible restoring lost or damaged data from off-site back up.
If we felt it was appropriate we would inform the police.

**Assessment of on-going 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 or damage of reputation 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 . We would also use the reporting tool in the IG toolkit website which is accessible once logged in.

**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.

## Confidentiality code of conduct for staff

### 1. Introduction

Everyone working for the practice is under a legal duty to keep patients' personal information confidential. Patients who believe their confidence has been breached may make a complaint to the practice and they could take legal action. In the case of a registered dental professional the patient could also make a complaint to the General Dental Council.

### 2. Purpose

This Staff Confidentiality Code of Conduct has been produced to ensure all staff members at Wall Heath Dental Practice are aware of their legal duty to maintain confidentiality, to inform them of the processes in place to protect personal information; and to provide guidance on disclosure obligations.

### 3. Scope

The code is concerned with protecting personal information about patients, although its content would apply equally to staff personal information. Personal information is data in any form from which a living individual could be identified; Although the Data Protection Act 2018 is only relevant to the personal information of living individuals, this code also covers information about deceased patients. The code applies to all staff including permanent, temporary, and locum members of staff.

### 4. Recognise your obligations

A duty of confidence arises out of the common law duty of confidence, employment contracts and for registered dental professionals, it is part of your professional obligations. Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal prosecution. So, make sure you do not:

- Put personal information at risk of unauthorised access;
- Knowingly misuse any personal information or allow others to do so;
- Access records or information that you have no legitimate reason to look at this includes records and information about your family, friends, neighbours and acquaintances.

### 5. Keep personal information private

Make sure you comply with the following staff guidelines which set out practical things you should do to keep personal information protected:

- Good record keeping (see Record management procedures);
- Appropriate use of computer systems (see Access control procedure);
- Secure use of personal information (see Information handling procedures);
- Reporting information incidents (see Incident management procedure);
- Using mobile computing devices.

### 6. Disclose with appropriate care

The Wall Heath Dental Practice will ensure that patients are adequately informed about the use and disclosure of their personal information in a leaflet. This will tell them why, how and for what purpose personal information is collected, recorded and used in the practice. You should ensure you are familiar with the patient information material and ensure you seek advice from the Information Governance lead Joanne Thompson if patients have questions you are unable to answer.

If you are authorised to disclose personal information you should ensure you do so in accordance with the **Information handling procedures** and you must only:

- Share with those with a legitimate right to see/hear the information;
- Transfer in accordance with the practice's secure transfer methods;
- Disclose the minimum necessary to provide safe care.

If you are authorised to disclose information that can identify an individual patient for non-healthcare purposes (e.g. research, financial audit) you must only do so if:

- You have the patient's explicit consent;
- The consent is written - to ensure there is no later dispute about whether consent was given.

Under the common law duty of confidence, identifiable personal information may be disclosed without consent in certain circumstances, these are:

- Where there is a legal justification for doing so, e.g. to comply with a statute;
- Where there is a public interest justification - i.e. where the public good that would be achieved by the disclosure outweighs both the obligation of confidentiality to the patient concerned and the broader public interest in the provision of a confidential service.

You must refer all requests for disclosure of personal information without the consent of the patient, including requests from the police, to the practice's Information Governance lead Joanne Thompson.

## Practice Information Security Policy

**1. General**

The Wall Heath Dental Practice 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).

- Joanne Thompson is designated as the Information Security Officer for the practice and;
- Lucy Thompson is the Caldicott Guardian
- Lucy Jeavons is the Data Protection Officer
- Mint Telecommunications Ltd are designated as the Technical Support Advisors

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) Passwords must be changed at the following intervals:
- Whenever you suspect it has been compromised
- Whenever a member of staff leaves
- Whenever a breach occurs
- At least every 6 months

(d) 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

(e) All computers and other devices must be locked to a secure screen-saver mode when not in active use

(f) Computers and other devices shall not be used so as to permit any unauthorised viewing or processing of personal data

(g) No personal data shall be copied, downloaded or transmitted to any device or storage medium other than those authorised by the Information Security Officer

(h) 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

(i) 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

(j) 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

(k) 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

**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.

**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 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

**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 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.

## Wall Heath Dental Practice 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 video 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 video footage of outside areas for practice security

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 Jill Thompson 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 Joanne Thompson.

**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 condiion 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 Joanne Thompson. 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.

## Wall Heath Dental Practice 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:

- Patient clinical and health data and correspondence.
- Staff employment data.
- Contractors' data.
- CCTV video data
- If you complete a survey on our website your IP address is stored

**Why we process Personal Data (what is the "purpose")**
"Process" means we obtain, store, update and archive data.

- Patient data is held for the purpose of providing patients with appropriate, high quality, safe and effective dental care and treatment.
- Staff employment data is held in accordance with Employment, Taxation and Pensions law; we have a separate more detailed privacy notice for our practice team.
- Contractors' data is held for the purpose of managing their contracts.
- IP addresses are stored to guard against misuse of the website.
- Video only CCTV footage of the outside of the building is recorded and overwritten after 30 days

**What is the Lawful Basis for processing Personal Data?**
The Law says we must tell you this:

- 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.
- We hold staff employment data because it is a **Legal Obligation** for us to do so.
- We hold contractors' data because it is needed to **fulfil a Contract** with us.
- If you complete a survey on our website, we will ask you to give **Consent**

**Who might we share your data with?**
We can only share data if it is done securely and it is necessary to do so.

- 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 is also shared, where appropriate, with regulatory authorities (such as the General Dental Council and Care Quality commission) and insurance companies (eg Denplan). Patient data is also stored for back-up purposes
- Employment data will be shared with government agencies such as HMRC.

**You have the right to:**

- Be informed about the personal data we hold and why we hold it.
- 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.
- Check the information we hold about you is correct and to make corrections if not
- Have your data erased in certain circumstances.
- Transfer your data to someone else if you tell us to do so and it is safe and legal to do so.
- Tell us not to actively process or update your data in certain circumstances.

**How long is the Personal Data stored for?**

- 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.
- We must store employment data for six years after an employee has left.
- 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?**
Joanne Thompson is our Information Governance Lead and Lucy Jeavons is our Data Protection Officer. They can both be contacted at Wall Heath Dental Practice.
You can complain in the first instance to us 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.

## Record Keeping Guidelines

**Create**
It is important that when a record is created it is Complete, Accurate, Relevant, Accessible, and Timely. This will ensure that the most up-to-date and relevant information is available at the point of need (timely).
Accurate, accessible and complete records will also protect the legal and other rights of the organisation, its patients, staff and any other people affected by its actions, and provide authentication of the records so that, if needed, the evidence derived from them is shown to be credible and authoritative.
Remember, once they are created, in whatever media form, they are public records and are covered by statute.

**Use**
Good quality records used within our practice will improve the way it operates as a business, and improve patient care and services.

Information security in all areas of our organisation is important, in order to protect patients and satisfy numerous laws (Data protection act, NHS Code of Practice).

The movement and location of records should be controlled in a secure way to ensure that a record can be easily retrieved at any time, remain secure in transit, whilst maintaining an auditable trail of record transactions.

Staff should only access the necessary patient data to complete their role. Access control measures are in place for both paper and electronic records. R4 permissions limit access to patient data appropriate to the staff role. Reception and administration staff have limited access to patient data so that are they are able to work effectively whilst maintaining patient confidentiality. R4 keeps an audit trail that provides evidence of anyone accessing electronic records without a business need to do so.

Records should remain on site – records, particularly patient health records should remain on site at all times, unless there is a clinical need for them to be transferred, and this must be done securely.

**Procedure for the retention and safe destruction of record cards**

Record cards of Patients who have been to the practice in the last 11 years and children up to the age of 25 are stored in the metal filing cabinets in the office which is kept locked.

For the purposes of the Consumer Protection Act 1987 record cards should be kept for at least 11 years for adults, and, for children, for 15 years or up to age 25, whichever is the longer. The record cards are periodically checked for any records that have reached this time limit and they are then safely destroyed by incineration, cross-cut shredding or by a confidential disposal service.

The practice is protected by a burglar alarm maintained by BAS Security Solutions

## Wall Heath Dental Practice Publication Scheme

The Freedom of Information (FOI) Act came fully into force on 1 January 2005. It was introduced to promote a culture of openness and accountability amongst public authorities by giving people rights of access to the information authorities hold. These rights should help better public understanding of how authorities carry out their duties, why they make the decisions they do and how they spend public money. Dental practices are now classed as public authorities under this act.

Under the Freedom of Information Act 2000 all public authorities are required to have and operate a publication scheme approved by the Information Commissioner. It is the intention of the Information Commissioner that all public authorities should adopt and operate the one model scheme that has been approved. This is a very general scheme based on the principal that all public authorities need to recognize the public interest in the transparency of the services provided for and paid for by the general public. It is a commitment to make information easily available to the public. For more information about model schemes go to the website of the Information Commissioner's office (the ICO) http://www.ico.org.uk/.

The ICO website provides further information about the Freedom of Information Act 2000, our obligations and your rights. It is also the place to look for information about the Data Protection Act 2018.

There is a document about the model scheme in Welsh on the ICO website.

**The Publication Scheme**
The Publication Scheme gives information about Wall Heath Dental Practice under the 7 classes of information we make available. If you cannot find the information you seek in this document, please write to us. This is not a complete list of publications since frequent changes are made.

The publication scheme only applies to the general dental services we provide under the National Health Service Act 2006 or the National Health Service (Wales) Act 2006. It does not include any information that is not held, is held for other purposes or would be exempt from release.

All of the information is available in hard copy from Joanne Thompson at the Wall Heath Dental Practice either immediately or within a few days if reprinting is required. The publications are all free unless otherwise indicated within each Class. Some of the information is available on our website www.wallheathdental.co.uk.

This guide will be reviewed at regular intervals and we will monitor its effectiveness.

**Your right to information**
As well as our published information, present and former patients of the practice have the right to access the personal information that we hold about them in accordance with the Data Protection Act 2018.

**Feedback**
We have produced this guide in order to comply with the Freedom of Information Act 2000. The purpose of the Act is to encourage organizations working for the public to be more open about the information they have. We welcome your views on additional classes of information which might be included and on the publications themselves. If you have any comments or suggestions about the scheme, please send them in writing to Joanne Thompson at the Wall Heath Dental Practice, 7 High Street Wall Heath, DY6 0HA.

**Classes of information**
We hold various types of information which we review, retain or dispose of according to NHS rules. Our information is classed into seven categories:

**Class 1 - Who we are and what we do**
This is current information only. The information is available in the practice leaflet available from Wall Heath Dental Practice reception free of charge and on our website at http://www.wallheathdental.co.uk.

**Who's who in the practice?**

| | | | |
|---|---|---|---|
| Joanne Thompson | Female | Part-time dentist | GDC first registration 1994 |
| Lucy Thompson | Female | Part-time dentist | GDC first registration 2006 |
| Jodi Read | Female | Part-time hygienist | GDC first registration 1988 |
| Carol Bradley | Female | Part-time hygienist | GDC first registration 1989 |
| Katie Wilson | Female | Part-time hygienist | GDC first registration 2008 |

Contact details:

| | |
|---|---|
| Address: | 7 High Street<br>Wall Heath<br>West Midlands<br>DY6 0HA |
| Phone | 01384 292666 |
| E-mail | info@wallheathdental.co.uk |
| Website | www.wallheathdental.com |

**Opening hours**
Monday 8:30 am – 12:30 pm & 1:30 pm – 5:00 pm.
Tuesday, Wednesday and Friday 8:30 am – 12:30 pm & 1:45 pm – 5:15 pm.
Thursday 9:30am – 1:30pm & 2:30pm – 6:00pm

Staffing structure
We are supported by a part-time nursing and reception staff team.

**Class 2 – What we spend and how we spend it**

Information about the following is available on request from our receptionist:

- The cost of NHS treatment
- Entitlement to exemption and remission from NHS dental charges
- Our private charges

Our income from the NHS derives from the contract that we have with NHS England Midlands to provide a fixed number of UDA (units of dental activity).
It also includes an allowance for CPD (Continuous Professional Development) and Clinical Audit.

*The current gross value of our contract is £118,028.42 Last year it was £112,794.74* *(updated 28/2/25)*

A proportion of all expenses incurred have to be paid out of this including staff wages, administration costs, heat, rates and insurance costs, cross infection control, clinical and special waste disposal, all materials and disposables, practice development funding, dentist further education and staff training, repairs and maintenance, servicing and replacement of equipment.

**Class 3 – What our priorities are and how we are doing**

We are regularly inspected by the Business Services Authority Dental Practice Board Division.
Since we are also a Denplan Excel practice we are inspected by a Denplan representative annually.
We comply with all current legislation and registered with the CQC in 2011.
The CQC inspected us in July 2024 and we met all the standards.

We hold internal audits on various aspects of patient care and administration.

We hope to be able to increase our contract with NHS England Midlands as necessary to continue to care for new patients.

**Class 4 – How we make decisions**
We have regular practice meetings with our staff. These, together with discussions between the partners, result in an on-going development of practice services.

**Class 5 – Our policies and procedures**
We have policies and procedures which ensure that the practice operates in a safe and efficient manner. These include:

- Health and safety policy;
- Complaints procedures (including those covering requests for information)
- Records management policies (records retention, destruction and archive);
- Confidentiality policy
- Data protection policy
- Record card security policy
- Infection control policy
- Equality and diversity policy
- Policies and procedures for handling requests for information
- Policies which safeguard patient safety, child protection and vulnerable adults
- Policies and procedures about customer service.

Copies of the policies are available from Joanne Thompson on request

**Class 6 – Lists and Registers**
We do not hold any lists or registers

**Class 7 – The services we offer**
We provide NHS general dental service to children and adults exempt from NHS charges.

The services provided under contract to the NHS include the full range of treatments necessary for dental health. We also provide sedation services and domiciliary visits where necessary.

We charge the current NHS charges for the band of treatment provided. Information regarding these charges is on our notice board in the reception area and a copy is available from our receptionist on request.
-We have a range of patient information leaflets available free of charge

**Further Information**
From January 2005 we are required by the Freedom of Information Act to respond to requests from the public to access recorded information that we hold. There are some exemptions to this right and it does not change the rights of our patients to have all of their personal information kept strictly confidential and available to them on request.
**Further information on the Freedom of Information Act is available from the following websites:**
https://ico.org.uk/
https://www.gov.uk/make-a-freedom-of-information-request/the-freedom-of-information-act

## National Data Opt-out Policy

Use this service to:
Choose if your confidential patient information is used for research and planning
Change or check your current choice
Your choice will be applied by:

- NHS Digital and Public Health England
- All other health and care organisations
- Any choice you make will not impact your individual care.

https://www.nhs.uk/your-nhs-data-matters/manage-your-choice/

## Emergency and Business Continuity Plan

The Practice has a detailed emergency and business continuity plan which is reviewed every 6 months or whenever there are significant changes to the building or working practices. Since it contains confidential information it is not appropriate to publish it within this manual

## Incident Management Procedures

**Introduction**
Ensuring personal information remains confidential and secure is everyone's responsibility and therefore, it is important to ensure that when incidents do occur, the damage from them is minimised and lessons learnt from them.

**Purpose**
The Incident Management Procedures set out how the Wall Heath Dental Practice will investigate and manage information incidents; and provide practice staff with guidelines on identifying and reporting information incidents including near-misses.
Where relevant they should be read in conjunction with the practice's Emergency and Business Continuity Plan.

**Scope**
The procedures apply to incidents that impact on the security and confidentiality of personal information.
These information incidents can be categorised by their effect on patients and their information:

- Confidentiality- unauthorised access, data loss or theft causing an actual or potential breach
- Integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information;
- Availability, e.g. records missing, misfiled, or have been stolen compromising or delaying patient care.

These procedures apply to all staff including permanent, temporary, and locum members of staff.

**Managing incidents**
The practice has assigned the role of **Incident Manager** to the Information Governance Lead **Joanne Thompson.**

Any actual or potential information incident in the practice will be assigned to one of the following categories, and investigated and managed accordingly.

1. **Report that patient confidentiality has been breached or put at risk**
   This could be reported by an affected patient, a relative; a member of the public or other staff:
   a. Interview the complainant to establish the reason for the complaint and why the practice is being considered responsible;
   b. Investigate according to the information given by the complainant;
   c. Record findings, e.g. unsubstantiated concern, suspected/potential breach, actual breach, etc.;
   d. Where necessary, provide written explanation to the patient with formal apology if warranted;
   e. Take and document appropriate action, e.g. no further action as there is no evidence that information was put at risk, advice/training, disciplinary measures, etc.

2. **Inadequate disposal of confidential material**
   This type of incident may lead to a breach of confidentiality and is likely to be reported by a patient affected, a member of the public, or a member of staff and could be paper, hard drive etc.:
   a. Investigate how the information left the practice by interviewing staff and contractors as appropriate
   b. Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g. breach of confidentiality, misuse of data
   c. Consider whether the patient(s) should be informed and where it is judged necessary, provide written explanation to the patient(s) with formal apology
   d. Record findings, e.g. potential breach, actual breach, evidence of misuse, etc.
   e. Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, etc.

3. **Attempted or actual theft of equipment and/or access by an unauthorised person**
   This type of incident may lead to a breach of confidentiality, the risk that information has been tampered with, or information not being available when needed:
   a. Check the asset register to find out whether equipment is missing
   b. Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base)

c. If the cause is external inform the police, ask them to investigate and keep them updated with your findings;
d. Interview staff and check the asset register to establish what data was being held and how sensitive it is;
e. Establish the reason for the theft/unauthorised access, such as:
    i. Items to sell;
    ii. Access to material to embarrass the practice;
    iii. Access to material to threaten patients (blackmail, stigmatization).
f. Consider whether there is a future threat to system security;
g. Inform insurers;
h. Review the physical security of the practice;
i. If there has been unauthorised access to the practice computer system:
    i. Ask the system supplier to conduct an audit to determine whether unauthorised changes have been made to patient records;
    ii. Consider whether any care has been provided to patients whose records have been tampered with;
    iii. Check compliance with access control procedures, e.g. ensure passwords haven't been written down, staff members are properly logging out, etc.
j. Consider the sensitivity of the data and the risk that it has been tampered with or will be misused, in order to assess whether further action is appropriate (e.g. warning patients);
k. If computer hardware or the core software has been stolen, inform system suppliers to enable restoration of system data to new equipment;
l. Record findings, e.g. potential breach, actual breach, evidence of tampering, compromised or delayed patient care, etc.;
m. Take and document appropriate action, e.g. physical security improvements, advice/training, disciplinary measures, etc.

4. **Computer misuse by an authorised user**

This includes browsing dental records when there is no requirement to do so; accessing unauthorised Internet sites; excessive/unauthorised personal use, tampering with files, etc.

a. Interview the person reporting the incident to establish the cause for concern;
b. Establish the facts by:
    i. Asking the system supplier to conduct an audit on activities by the user concerned;
    ii. Interviewing the user concerned.
c. Establish whether there is a justified reason for the alleged computer misuse;
d. Consider the sensitivity of the data and the risk to which the patient(s) have been exposed, e.g. breach of confidentiality; the risk information may have been tampered with; and consider whether the patient(s) should be informed;
e. Record findings, e.g. breach of confidentiality, evidence of tampering, fraud, carrying on a business, accessing pornography, etc.;
f. Take and document appropriate action, e.g. no action as allegation unfounded, training/advice, disciplinary measures, etc.

**Reporting incidents to external organisations**

Serious information incidents, i.e. those categorised as level 3 - 5 in the table below are reported to the Area Team and the Information Commissioner. They should also be reported using the incident reporting tool on the IG Toolkit website. This is accessed after logging in with the practice details

| Reporting categories for information incidents | | | | | |
|---|---|---|---|---|---|
| **0** | **1** | **2** | **3** | **4** | **5** |
| Minor breach of confidentiality affecting one patient. | Potentially serious breach. Less than 5 patients affected or risk assessed as low, e.g. files were encrypted. | Serious potential breach and risk assessed high, e.g. unencrypted records of up to 20 patients. | Serious breach of confidentiality, e.g. up to 100 patients affected. | Serious breach with either particular sensitivity, e.g. sexual health details, or up to 1000 patients affected. | Serious breach with the potential for ID theft of over 1000 patients affected. |
| Minimal discernible effect on the practice - media interest unlikely. | Damage to staff member's reputation. Possible media interest, e.g. celebrity involved. | Damage to the practice's reputation, some local media interest that may not go public. | Damage to the practice's reputation, low-key local media coverage. | Damage to the practice's reputation, local media coverage. | Damage to the NHS' reputation, national media coverage. |

**Lessons learned**
The practice maintains a register of all incidents occurring within the organisation. This register of incidents and the resulting actions taken will inform the other policies and procedures within the practice.

All registered incidents are re-evaluated after a 6 month period to assess the effectiveness of the implemented actions in ensuring that either the type of incident is no longer being reported or the volume of those types of incidents has reduced. If there is no change in the volume of each type of incident the practice partner(s) are alerted and appropriate action taken.

To provide staff with an example of what could occur, how to respond to such events and how to avoid them, previous incidents are used in security and confidentiality training sessions.

**Note for more serious incidents:**
There is now an IG Toolkit Incident Reporting Tool available and new reporting categories. Guidance on using the tool can be found at:

*https://www.igt.hscic.gov.uk/KnowledgeBaseNew/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance_V5%201%20290515_Final_Publish.pdf*

## Information Governance Policy

**Introduction**
Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

**Purpose of the policy**
This Information Governance policy provides an overview of the practice's approach to information governance; a guide to the procedures in use; and details about the IG management structures within the dental practice.

**The practice's approach to Information Governance**
The Wall Heath Dental Practice undertakes to implement information governance effectively and will ensure the following:

- Information will be protected against unauthorised access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Information will be supported by the highest quality data;
- Regulatory and legislative requirements will be met;
- Business continuity plans will be produced, maintained and tested;
- Information governance training will be available to all staff as necessary to their role;
- All breaches of confidentiality and information security, actual or suspected, will be reported and investigated.

**Procedures in use in the practice**
This Information Governance policy is underpinned by the following procedures:

- Records management procedure that set outs how patient dental records will be created, used, stored and disposed of;
- Access control procedure that sets out procedures for the management of access to computer-based information systems;
- Information handling procedure that sets out procedures around the transfer of confidential information;
- Incident management procedure that sets out the procedures for managing and reporting information incidents;
- Business continuity plan that sets out the procedures in the event of a security failure or disaster affecting computer systems.

**Staff guidance in use in the practice**
Staff compliance with the procedures is supported by the following guidance material:

- Records management: guidelines on good record keeping;
- Staff confidentiality code of conduct: sets out the required standards to maintain the confidentiality of patient information; obligations around the disclosure of information and appropriately obtaining patient consent;
- Access control: guidelines on the appropriate use of computer systems;
- Information handling: guidelines on the secure use of patient information;
- Using mobile computing devices: guidelines on maintaining confidentiality and security when working with portable or removable computer equipment;
- Information incidents: guidelines on identifying and reporting information incidents.

**Responsibilities and accountabilities**
The designated Information Governance lead for the practice is Joanne Thompson.
The key responsibilities of the lead are:

- Developing and implementing IG procedures and processes for the practice;
- Raising awareness and providing advice and guidelines about IG to all staff;
- Ensuring that any training made available is taken up;
- Coordinating the activities of any other practice staff given data protection, confidentiality, information quality, records management and Freedom of Information responsibilities;
- Ensuring that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott Principles;
- Monitoring information handling in the practice to ensure compliance with law, guidance and practice procedures;

- Ensuring patients are appropriately informed about the practice's information handling activities

The day to day responsibilities for providing guidance to staff will be undertaken by Joanne Thompson.

**Our Data Protection Officer is Lucy Jeavons.**

The owners of the practice are responsible for ensuring that sufficient resources are provided to support the effective implementation of IG in order to ensure compliance with the law, professional codes of conduct and the NHS information governance assurance framework.

All staff, whether permanent, temporary or contracted, and contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy and the procedures and guidelines produced to support it.

## Guidance on Retention of Records in Dental Practice

The RMCoP (Records management code of practice for health and social care)

| Data Category | Start of Retention Period | Recommended Minimum Length of Retention | Comment |
|---|---|---|---|
| NHS GDS patient notes not included below | Date of last entry | 11 years | As recommended by NHS |
| Patients undergoing treatment for cancer | Date of diagnosis | 30 years or 8 years post mortem | |
| Patients with long term or recurrent disease | Date of last entry | 30 years from discharge | Could include chronic unresponsive periodontal disease |
| Clinical Audit | Date of creation | 5 years | Where personal data is identifiable |
| Patients where serious incidents occurred | Date of incident investigation closure | 20 years | |
| Patients where minor incidents occurred | Date of incident investigation closure | 10 years | |
| Patients involved in complaints or litigation | Date of resolution or completion of litigation | 10 years after closure | |
| FP17 bands 1.2, 2 & 3 | Date of completion | 11 years | As recommended by NHS |
| PR Forms | Date of completion | 2 years | As recommended by NHS |

- See: https://digital.nhs.uk/information-governance-alliance/
- https://transform.england.nhs.uk/information-governance/guidance/records-management-code/

## Data Retention Schedule

| 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 | Currently we destroy everything – there is no record on card of | 30 years | IGA RMCoP |

| | | | | |
|---|---|---|---|---|
| | | these conditions so no way of identifying them | | |
| Clinical audit records | Date of audit | 5 year | 5 years | Where identification of individual patients is possible (IGA RMCoP |
| Staff records, Occupational Health records | Date of leaving | 6 years | 6 years | IGA RMCoP |
| Staff records: radiological dosimetry results | Date of record | N/A | 40 years | IRR legislation 2017 |
| Staff records: timesheets | Date of creation | 2 years | 2 years | IGA RMCoP |
| Contracts for services | Date of cessation of contract | 6 years | 6 years | e.g. self-employed staff or maintenance contracts (Statute of Limitations) |
| Financial records | Date of completion of record | 6 years | 6 years | HMRC recommendation: look-back period |
| Telephone recordings | Date of recording | N/A | | Many recordings will be transcribed and over-written in a short period – possibly one week, but in the event of a serious issue should be retained for disclosure |
| Subject Access Requests | Date of supply of information | 3 years | 3 years | IGA RMCoP |
| CCTV records | Date of recording | N/A | 30 days | Duration of time necessary e.g. to report and investigate crime |
| Software licences | Date of inception | Lifetime of software | Lifetime of software | Data must be supplied to data controller and erased when contract expires |
| Significant incident log | Date of incident | Major – 20 years<br>Minor – 10 years | Major – 20 years<br>Minor – 10 years | IGA RMCoP<br>Non-clinical – 12 years advised |

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

## Staff Training Documents

This is a list of the staff training documents in use. The full documents are contained in Wall Heath Dental Practice Data Protection Handbook - Policies and Risk Assessments Specific to Wall Heath Dental Practice. As well as being familiar with these procedures all staff are required to undertake Data Security Awareness CPD every year.

- Information Handling Procedures
- Preventing and dealing with unauthorised access
- Routine Flow Mapping
- Confidentiality training for the practice team
- Data protection code of practice
- Practical working guide: Dos & Don'ts
- Guidelines on identifying and reporting information incidents
- Guidelines on the appropriate use of computer equipment
- Guidelines on the secure use of personal information
- Guidelines on the use of mobile computing equipment
- Payment card security policy and staff training
- Data Awareness training (e-Learning for Healthcare website)
- To use NHS mail to securely send and receive documents to non-NHS mail users

Clinical Record Log of decision process for destruction added 18/9/23
Not destroyed after 11 years because:

| | |
|---|---|
| Complex dental case<br>- implants<br>- full mouth treatment<br>- periodontal disease<br>- orthodontic treatment | |
| Lack of capacity to consent | |
| Vulnerable/safeguarding concern | |
| Registered disability | |

## Risk Assessments, Action Plans and Wall Heath specific information

This is a list of the risk assessment carried out and action plans introduced as a result. The full documents are contained in Wall Heath Dental Practice Data Protection Handbook - Policies and Risk Assessments Specific to Wall Heath Dental Practice. These risk assessment are reviewed at least every 12 months, discussed at management and practice meetings and new action plans devised.

- Action plan for improving security of premises and information
- Information Governance Improvement Plan
- Wall Heath Dental Practice Information asset register
- Data Security Improvement Plan.
- Information flow mapping risk assessment
- Physical security risk assessment and action plan
- Security Risk Assessment and action to be taken if unauthorised access is suspected
- List of staff and third parties with access to patient data
- Legitimate Interest Assessment for holding patient data
- Legitimate Interest Assessment for holding employee and contractors data
- Wall Heath Dental Practice Data Audit

## Forms and Posters for printing

This is a list of the forms and monitoring sheets used on a day to day basis.
The full documents are contained in Wall Heath Dental Practice Data Protection Folder
These forms are reviewed at least every 12 months to fit in with current practice

- Asset control form
- Data protection principles poster for display in staff room
- Wall Heath Dental Practice Information Governance Incident Register
- Data Protection Breach Notification Form
- Compliance Monitoring