Confidentiality Policy

Purpose

The purpose of this document is to ensure all staff members at the 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.

Introduction

Everyone working within the practice or across the wider business has a legal obligation to maintain the confidentiality of patients' personal information. Patients who believe their confidence has been breached may make a complaint to the practice, and they could take legal action or report it to the ICO. In the case of a registered dental professional, the patient could also make a complaint to the General Dental Council, which, in worst-case scenarios, may end in erasure from the GDC register.

This policy is concerned with protecting personal information about patients, although its content would apply equally to staff personal or business-sensitive information.

Personal information is data in any form (paper, electronic, tape, verbal, etc.) from which a living individual could be identified, including:

- Name, age, address, and personal circumstances, as well as sensitive personal information like race, health, sexuality, etc.
- Information regarding appointments
- Information regarding medical histories
- Information regarding finances, including any bad debts.

Although the Data Protection Act 2018 is only relevant to the personal information of living individuals, this code also covers information about deceased patients. This policy applies to all staff, including permanent, temporary, and locum staff members.

Data Protection Roles and Responsibilities

The practice has appointed a Data Protection Officer who is responsible for overseeing compliance with UKGDPR and the Data Protection Act 2018, managing data protection queries, and acting as a point of contact for the ICO.

All staff are responsible for maintaining confidentiality and must comply with this policy at all times.

As a practice providing NHS services, a Caldicott Guardian has been appointed or assigned responsibility for ensuring patient information is shared appropriately and securely in line with Caldicott Principles.

Confidentiality

Under the Data Protection Act 2018 and UK GDPR, dental practices must keep personal data about their patients safe and secure and ensure it is only accessed by persons who need to see it for the purposes of providing safe, effective care.

Registered dental professionals have an ethical and legal duty to keep all patient information confidential.

Dental practices are also required to ensure that they do not 'advertise' to other patients or the public that a particular person is a patient of the practice or that they have had appointments or have appointments due. This means that day lists, appointment cards that identify the patient and record cards must not be seen by other patients in the practice. It is also important that confidential telephone calls that name a particular patient are not held in earshot of other patients. Messages should not be left with a 3rd party confirming or cancelling appointments.

Caldicott Principles

The Caldicott Principles provide a framework for ensuring that patient-identifiable information is shared appropriately and securely.

All NHS organisations must have an appointed Caldicott Guardian. While this requirement does not typically apply to independent dental practices, there should still be a designated individual within the practice who is responsible for overseeing patient confidentiality and ensuring that information is shared appropriately when necessary.

HW Dental Centre has appointed a Caldicott Guardian who is responsible for safeguarding patient information and ensuring appropriate use. They will provide advice on whether disclosures of information are appropriate and ensure compliance with the Caldicott Principles.

Our Caldicott Guardian is Kiril Stanilov.

The Caldicott Principles

- Principle 1: Justify the purpose for using the confidential information.
- Principle 2: Use confidential information only when it is necessary
- Principle 3: Use the minimum necessary confidential information
- Principle 4: Access to confidential information should be on a strict need-to-know basis
- Principle 5: Everyone with access to confidential information should be aware of their responsibilities
- Principle 6: Comply with the law
- Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Principle 8: Inform patients and service users about how their confidential information is used.

Disclosing Patient Information

Personal information relating to a patient should only be shared with third parties where the patient has given consent or in exceptional circumstances (GDC Standards 4.3).

Patient information will only be disclosed to third parties where:

- The patient has given valid consent, or
- There is a legal obligation or overriding public interest.

Examples of where information may be shared without consent include:

- In safeguarding concerns, where it is not possible to gain consent, a referral needs to be made to the local authority or to the police.
- Where information has been ordered by a court or by a coroner, or where a court order has requested information, only the minimum amount of information should be disclosed.

Only the minimum necessary information will be shared.

Where there is any uncertainty regarding disclosure without consent (and where there is no immediate safeguarding risk), advice should be sought from the practice's indemnity provider prior to releasing the information where appropriate. Safeguarding concerns should not be delayed in order to seek such advice.

The Importance of Confidentiality

The relationship between clinician and patient is based on the understanding that any information revealed by the patient to the clinician will not be divulged without the patient's consent. Patients have the right to privacy, and it is vital that they give clinicians full information on their state of health to ensure that treatment is carried out safely and effectively. The intensely personal nature of health information means that many patients would be reluctant to provide the clinician with information if they felt the information would be passed on.

Care must be taken to ensure that confidentiality is never breached, even to the most minor degree, in the use of social media or websites (GDC Standards 4.2.3).

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 their professional obligations. Breaches of confidence and inappropriate use of records or computer systems are serious matters that 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.

Communication and Reception Confidentiality

Staff must take care when handling patient information in all communications.

- Verify patient identity before disclosing information
- Avoid discussing confidential information in public areas

- Do not leave detailed voicemail messages without consent
- Patient information must not be disclosed to third parties without appropriate authorisation
- Ensure emails are sent securely and to the correct recipient.

Extra care must be taken in reception areas to ensure conversations cannot be overheard.

Training

All staff will receive training in confidentiality, data protection and information governance at induction and at regular intervals thereafter.

GDC standards guidance

Dental care professionals have an ethical and legal duty to be familiar with and comply with the GDC's standards and guidance. All practice team members must also follow this guidance and ensure patient confidentiality. Copies of this publication in full are available as PDF downloads from the GDC's website at www.gdc-uk.org

4.2 You must protect the confidentiality of patients' information and only use it for the purpose for which it was given.

4.2.1 Confidentiality is central to the relationship and trust between you and your patients. You must keep patient information confidential. This applies to all the information about patients that you have learnt in your professional role, including personal details, medical history, what treatment they are having and how much it costs.

4.2.2 You must ensure that non-registered members of the dental team are aware of the importance of confidentiality and that they keep patient information confidential at all times.

4.2.3 You must not post any information or comments about patients on social networking or blogging sites. If you use professional social media to discuss anonymised cases for the purpose of discussing best practice, you must be careful that the patient or patients cannot be identified.

Appendix 1 – Standard Operating Procedure: Confidentiality

Purpose

To ensure all patient information is handled securely, lawfully, and confidentially in line with:

- UK GDPR & Data Protection Act 2018
- GDC Standards (Principle 4)
- CQC Regulations (Reg 10 & 17)

Scope

This SOP applies to:

- All staff (clinical, non-clinical, temporary, locum)
- All patient information (electronic, paper, verbal, images)

Responsibilities

- **All Staff**
  - Maintain confidentiality at all times
  - Comply with the Data Protection Act 2018, UK GDPR and information governance requirements
- **Practice Manager/Data Protection Officer**
  - Oversee compliance
  - Manage data breaches and SARs
- **Clinicians**
  - Ensure appropriate information sharing for patient care.

Key Rule: Need-To-Know Only

- Only access information required for your role
- Never access records out of curiosity
- Keep passwords secure and private

Daily Practice

Do:

- Check patient identity before sharing information
- Position screens so they are not visible to patients
- Lock computers when unattended
- Store paper records in locked cabinets
- Speak discreetly at the reception
- Use secure email (NHSmail) where required
- Share only the minimum necessary information

Do Not:

- Discuss patients in public areas
- Leave records or screens unattended
- Share passwords or login details
- Send patient data via WhatsApp/social media
- Leave detailed voicemail messages without consent

Sharing Information

You may share information:

- With patient consent
- If required by law (e.g. safeguarding, court order)

Always:
- Share the minimum information necessary
- Seek advice if unsure (without delaying urgent safeguarding referrals)

Patient Rights (SARs) – see the Subject Access Request Form for more information

- Patients can request access to their records
- Must be completed within 1 month
- Refer requests to Practice Manager/DPO

Data Breaches

Examples:

- An email containing confidential information was sent to the wrong recipient
- Lost or misplaced records
- Unauthorised access to patient data
- Loss or theft of paper records, laptops, USBs, or mobile devices containing patient data
- Disposing of confidential waste incorrectly (e.g. not using confidential waste bins or shredding)

What to do:

- Report immediately to the Practice Manager/DPO
- Follow the Data Breach Flowchart

Social Media

- Never share patient information
- Images require written consent
- Patients must not be identifiable

Confidentiality must never be compromised. If unsure — seek advice before sharing information.

Document Control

Title:	Confidentiality Policy
Author/s:	DCME Team

Owner:	DCME Team
Approver:	DCME Team
Date Original Approved:	25.3.23
Review Date:	May 2026
Next Review Date:	12-18 months from the above date

Change History				
Version	**Status**	**Date**	**Author / Editor**	**Details of Change** (Brief detailed summary of all updates/changes)
0.1	Final	25.3.23	PG	Complete re-write of policy, updated guidance.
0.2	Final	21.03.24	HD	Minor amendments. Addition of information regarding the Caldicott Principles and disclosing information to third parties.
0.3	Final	07.25	HD	Added information about a Caldicott Guardian and space to include their details if applicable.
0.4	Final	May 2026	HD	Added roles and responsibilities and information on maintaining confidentiality at reception. Also added a short SOP for ease of use.

The latest approved version of this document supersedes all other versions, upon receipt of the latest approved version all other versions should be destroyed, unless specifically stated that previous version(s) are to remain extant. If in any doubt, please contact the document Author.

Approved By: Kiril Stanilov, Elena Belichka-Stanilova
Date Published: 17/11/2026