



For Church Road Dental.

The Practice Manager is Katie Lockyear.

The Senior Information Risk Officer (SIRO) is the Practice Owner Pritesh Vithlani, who is responsible for overseeing data security measures and risk management.

The Information Governance Lead (IG Lead), Katie Lockyear, is responsible for managing information handling, training, and compliance in accordance with these procedures.

The Practice has appointed a Caldicott Guardian, Katie Lockyear/ Pritesh Vithlani, to advise and support staff on the sharing and disclosure of person-identifiable patient information.

The Practice has appointed, Katie Lockyear, as the Data Protection Officer (DPO) to monitor data protection compliance in line with these procedures, and provide independent advice on matters such as DPIAs, data breaches, and privacy rights requests.

These are the procedures for data protection and information governance, to meet the requirements of the UK GDPR, the Data Protection Act 2018 and professional standards. Refer to the Data Protection Overview (M 216) and Data Protection and Information Security Policy (M 233-DPT).

General information about the data we process:

Details of the personal data and special category data that we hold are in our Privacy Notice for Patients (M 217T) and Privacy Notice for Staff (M 217TS).

How we hold personal data	Personal data is held in digital form on the practice computer / in cloud servers or services / backed up online
How we collect personal data	We collect personal data directly from team members or patients by phone, in person, by email, using online forms, from referrals
How we hold special category data	Special category data is held in digital form on the practice computer / in cloud servers or services / backed up online
How we collect special category data	We collect special category data directly from team members or patients, by phone, in person, by email, using online forms, from referrals

Lawful basis for processing data

It is necessary to have a valid lawful basis in order to process personal data. Of the six available lawful bases for processing no single basis is 'better' or more important than the others. We have determined our lawful basis before we began processing, and we document it here.

When we process criminal conviction data or data about offences we have identified both a lawful basis for general processing and an additional condition for processing this type of data. When recruiting team members, it is a requirement to obtain a criminal record check, but we take care to handle the data appropriately, see the Information Security section below for further information.

The lawful basis for processing data at the practice is found in our Privacy Notice for Patients (M 217T), Privacy Notice for Children (M 217TC), and Privacy Notice for Staff (M 217TS).

Consent

The practice offers real choice and control to all individuals. Our consent procedures put individuals in charge to build customer trust and engagement. Our consent for marketing requires a positive opt-in, we



don't use pre-ticked boxes or any other method of default consent. We make it easy for people to withdraw consent and tell them how and keep contemporaneous evidence of consent. Consent to marketing is never a precondition of a service.

All new patients are asked to complete [a Communication Consent Form (M 217RA)/a medical history containing marketing opt in questions]. When applicable, we ask patients to complete a Consent for Clinical Photography (M 217RB) form.

Ongoing consent for processing data for marketing purposes is managed [by email/by post].

Managing individual's rights

To manage individual's rights, we use the following procedures:

- Patients or non-patients may contact us by phone, email or in person to ask us take actions on their data as described above
- The Practice Manager will respond to the individual, using the same method of communication used by the individual to contact the practice, within 3 working days confirming that their request is being processed
- If a patient requests a copy of their clinical notes or a non-patient requests a copy of their personal data, they will normally be provided with a copy free of charge
- For any additional copies or excessive requests, we will charge a reasonable fee of up to [£10] for digital records and [£50] for paper records
- The data request will usually be completed within one month of receiving the request
- If there are delays due to a complex request the patient will be contacted within 1 month of making the request with the reasons for the delay and the expected delivery date, which must be within 3 months
- In the communication to the individual, they will be informed where to find the Privacy Notice for Patients (M 217T), Privacy Notice for Staff (M 217TS) or the Privacy Notice for Children (M 217TC) [on the practice website or by contacting the practice]
- Once the data request has been fulfilled the Practice Manager will enter the details on [the spreadsheet called Data Requests Record (M 217RX)], and if the individual is a patient, the details will also be recoded on the clinical record
- Each year, the Data Requests Record is checked during the iComply activity on data protection

Right of access for children

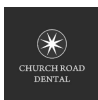
Even if a child is too young to understand an access request, it is still their personal data and does not belong to anyone else such as a parent or guardian. When handling a request for information about a child we always consider if the child is mature enough to understand their rights. If they do, then we consider responding directly to the child rather than the parent. When a child makes a request, they are provided with a copy of the Privacy Notice for Children (M 217TC) [or told where to access it on the website].

Information about a child may be released to a person with Parental Responsibility, taking into account the best interests of the child. All mothers and most fathers have this responsibility and parents do not lose it if they divorce, although it can be removed by a court. When in doubt about parental responsibility, proof of identity and evidence is requested. Note: For more information on how a parent can prove that they have parental responsibility see the [gov.uk advice page](https://www.gov.uk/advice-page).

Access requests and mental capacity

For patients who lack the mental capacity to manage their own affairs, an attorney or other person with a Lasting Power of Attorney, or someone appointed by the courts will have the right to access information about the person they represent and make decisions on their behalf. Proof of identity and evidence of power of attorney or court order is always requested. The same applies to a person appointed to make decisions by the Court of Protection in England and Wales.

Right to be informed



We provide 'fair processing information', through our Privacy Notice for Patients (M 217T), Privacy Notice for Children (M 217TC), and Privacy Notice for Staff (M 217TS), which provides transparency about how we use personal data. The Privacy Notices are available [on our website at www.website.co.uk/privacynotice/ from the practice in printed form / other method].

We also provide on request the Patient Leaflet on Personal Information (M 217P), which is available [from the practice in printed format / from the practice website].

Data processors and contracts

Data processors are third parties who processes personal data on our behalf. We have identified who our data processors are, where they store their data and, if it is outside of the EU, that they have suitable arrangements to secure our data that meets UK GDPR requirements.

In response to the invalidation of the EU-US Privacy Shield in 2020, we have reviewed all our processing agreements to limit the transfer of our data to within the EU wherever possible. Where transfers to the US continue, we have performed a written assessment for every company and ensured that adequacy regulations or appropriate safeguards are in place.

Appropriate safeguards include:

- A legally binding and enforceable instrument between public authorities or bodies
- Binding Corporate Rules (BCRs)
- Standard contractual clauses (SCCs)
- An approved code of conduct
- Certification under an approved certification scheme
- Contractual clauses authorised by the ICO
- Administrative arrangements between public authorities or bodies

Where transfers are made outside the UK or EU, the practice has performed a written assessment for every company and ensured that adequacy regulations or appropriate safeguards are in place.

We have an appropriate contract with all of our data processors, we use the Model Contract for Data Processor or Joint Data Controllers (M 217UA) for smaller companies when the company does not provide their own contract. Alternatively, the processor will send us their own contract. We have a link to the relative terms for the bigger companies such as Dropbox, Agilio or Microsoft who are unable to send us individual agreements.

Companies who store and process our data	▪ Company - Radiation protection services ▪ Company - Berg and williams - company- Software of excellence ▪ Dental laboratories - Pyramid, AK labs, BDS, AESTHETIC WORLD, SITHA, SUN DENTAL, S4S, DESIGN. ▪ Computer support companies - Comart ▪ ▪ Self-employed associate/hygienist/therapist/clinical dental technician 1 ▪ Self-employed associate/hygienist/therapist/clinical dental technician 2 ▪ Note: Companies that store our data include: Agilio, Online backup companies such as Data Barracks, Cloud storage such as iCloud, Microsoft 365, Google Docs, Dropbox, online software companies such as iComply or practice management software ▪ Our self-employed associates/hygienists/therapists/clinical dental technicians, are data processors
--	--

Digital data stored and processed within the UK or EU	We have contracts with all of the companies listed below who store data on our behalf. We either have their contract, a link to their relevant terms, or in the case of our self-employed associates/hygienists/therapists/clinical dental technicians, they have signed our Contract for Data Processors (M 217UA): ▪ Agilio, https://www.agliosoftware.com/, their terms as data processor are to be found at https://agliosoftware.com/terms/ ▪ Our self-employed associates/hygienists/therapists/clinical dental technicians, who we allow to process data on our behalf have signed the Model Contract for Data Processor or Joint Data Controllers (M 217UA)]
Digital data stored and processed outside of the UK or EU	We have contracts with all of the companies listed below who store or process data on our behalf, have performed a written assessment for every company and ensured that adequacy regulations or appropriate safeguards are in place. ▪ [Invisalign, Invisalign process data we control in line with their Privacy Policy and Binding Corporate Rules which set out their framework to satisfy the standards contained in European data protection law and, as a result, provide an adequate level of protection for all personal information used and collected in Europe and transferred outside Europe. These Binding Corporate Rules have been reviewed by us and can be viewed here.] ▪ [Company 2, process data we control in line with their Privacy Policy and [insert explanation of assessment performed and adequacy regulations or appropriate safeguards in place]

Data protection by design

We implement technical and organisational measures to integrate data protection into our processing activities. Our data protection and information governance management systems and procedures take data protection by design as their core attribute to promote privacy and data compliance. Data Protection Impact Assessments (DPIAs) are an integral part of taking a data protection by design approach.

Records

We keep records of processing activities for future reference.

Data Protection Impact Assessment (DPIA)

A Data Protection Impact assessment (DPIA) is a way to analyse new data processing and help identify, and minimise, data protection risks systematically and comprehensively. As required under UK data protection regulation, we will consider undertaking a DPIA before beginning any type of processing that is “likely to result in a high risk” to data subjects.

We will consider whether we need to carry out a DPIA if we plan to:

- Use systematic and extensive profiling with significant effects (for example, this might include introducing a new type of e-recruiting software which make decisions without any human intervention)
- Process special category or criminal offence data on a large scale (for example, this might include moving a large number of patient records between digital systems)
- Systematically monitor publicly accessible places on a large scale (for example, the introduction of



- a CCTV camera on practice property which monitors a busy pedestrian area)
- Introduce or change our offsite storage of paper records
- Create a new record destruction process
- Use or change patient portals
- Use or change cloud solutions

If we consider that a DPIA may be required, we will follow the Information Commissioner Office's guidance, using their [DPIA template](#).

3-Step Backup Procedure

We use three-step backup procedure:

1. Local backups of important files and data using internal harddrives
2. Cloud (Internet) backup using [Databarracks] for a backup of our complete server
3. Network Attached Server (NAS) drive located [at the practice owner's home] for a backup of [all essential files] **OR** [our complete server]

All backups are encrypted and password protected for security.

1. Local backups of files and data

- All backups are encrypted
- Data is backed up every day using an external drive
- Backups are kept in a locked, fireproof safe at the practice
- At the end of each day the reception removes the relevant [external drive] backup from the safe, places it in the computer and runs the backup utility (or the computer will run it automatically at the end of the day)
- When the backup is complete the Practice Manager puts the backup in the fireproof safe and signs the Computer Backup Log (G 135A).
- Local backups are labelled as follows:
 - Monday/Friday
 - Tuesday/Thursday
 - Wednesday/Saturday
 - Offsite Monthly A
 - Offsite Monthly B

2. Cloud (Internet) backup

- We use a [Databarracks] to backup [all essential files/our complete server] on a daily basis
- Each week the Practice Manager checks the status of the backup and records this on the Computer Backup Log (G 135A)

3. Network Attached Server (NAS) drive backup

- We use a NAS drive to backup [all essential files/our complete server] on a daily basis
- Each week the Practice Manager checks the status of the backup and records this on the



Computer Backup Log (G 135A)

Information security

We have appropriate security to prevent the personal data we hold being accidentally or deliberately compromised. It includes technical security, physical security and the plan for appropriate response swiftly and effectively. To meet this requirement we have policies, procedures, risk assessments and planning which we review annually in iComply. Our approach to information security includes:

- Backup Procedures and Software (Log G 135)
- Subcontractor's Confidentiality Agreement (M 217F)
- Information Asset Log (M 217G)
- Mobile Equipment Terms and Conditions (M 217I)
- Compliance Monitoring Form (M 217K)
- Computer and Software Access Log (M 217L)
- Security Risk Assessment (M 217M)
- Business Impact Analysis (M 217N)
- Disaster Planning and Emergency Procedures (M 255)
- Data and Cyber Security Test Log (M 217X)

Electronic security

This electronic security section applies to desktop computers, laptop computers, tablets and smartphones. In networked computer systems it also applies to servers. The IG Lead is also responsible for allocating responsibility to keep any Internet router's software up to date.

Phishing

Team members are aware to **never click a link in an email unless they are sure of the sender**. A common way for cyber-criminals to obtain usernames and passwords is by sending an email that looks like it originates from a well-known bank or other service provider such as PayPal or Netflix. It will have a link that says, 'click here to reset your password' and usually has a strong message to drive the action such as 'take action now, account suspended'.

Inadvertently clicking on an unknown link may install malware on a device or computer, this is how many ransomware attacks are perpetrated. When the link is clicked the 'ransomware' may encrypt the computer rendering it useless unless you pay a large amount to the criminals who have sent you the malware. There are many variations of this type of cybercrime and to minimise the risk of it happening team members:

- Will only log onto sites using the original website of the company concerned, and never from a link in an email
- Will never click on links in emails unless they are sure of the sender

Requests for money

There are many ingenious ways that money can be stolen using email. These include:

- An email that seems to come from a friend who is in trouble
- An email that requests a bill to be paid to a different account than usual, or that ask for a fund transfer for any reason
- Emails that appear to come from a manager, requesting transfer of funds
- Emails that ask you to reset bank usernames and passwords
- Emails that ask for your personal details such as date of birth

Whenever an email like this is received, the team member will contact the sender, in person by telephone to confirm. The team member will only use the telephone number that they can confirm is the correct phone number of the supposed sender.



Important tasks

All team members must:

- Weekly
 - Update virus definitions of their devices and carry out a virus scan
 - Other
- Monthly
 - Check that all of their software is up to date, this includes the operating system, e.g. Windows, IOS or Android, and software such as Microsoft Word
 - Other

The IG Lead must:

- Monthly
 - [If using a multi computer anti-virus such as Sophos check the main panel for alerts and other important information:
 - That the users are current, that users aren't duplicated and that people who have left have been removed
 - That users have all of their devices listed under the user
 - That all computers, laptops and work phones have anti-virus installed, if not install it
 - That all computers, laptops and work phones have carried out a recent virus scan if not inform the user to do so]
 - [If each computer and mobile equipment has stand-alone virus protection, check that the latest virus definitions have been updated and scans have been completed on all equipment]
 - Check that the Network, Computer and Software Access Log (M 217L) is up to date
 - [If there are servers, check that the server software such as MS Small Business Server and software such as MS Word updates have been installed]
 - [Check the status of backups and the Computer Backup Log (G 135A)]
- 6-Monthly
 - Check that any Internet routers do not have the default admin password and have the latest software (often called firmware) installed
 - Update internet router and firewall firmware
 - Check that the network does not have any default admin passwords
 - Carry out a test restore of the backup/or ask your IT provider to carry it out for you
- Annually
 - Test of Data and Cyber Security aspects of our Disaster Planning and Emergency Procedures (M 255) (See below)

Password type and storage - notes for reference

The theory of using upper and lower-case letters mixed with numbers and special characters was invented by Bill Burr. Unfortunately, hackers have designed their password cracking software to 'crack' this type of password so they are no longer secure. He now advises use of four unrelated words such as 'moon rapport deckchair towel'.

Agilio recommends that all computer users install a password manager such as Dashlane, which helps the user easily manage different passwords for each login. It also completes name and address details or credit card details into a website form saving the user time. Some people are concerned that password managers may be hacked, however as far as Agilio is aware, this hasn't happened and we successfully use Dashlane.



The password rules for team members:

- Ensure all default passwords are changed after the first login
- Only use passwords where they are really needed
- Use [1 Password/Dashlane/Keeper/Other technical solution] to store and manage their passwords
- Are only asked to change their passwords when there is an indication of suspicion or compromise
- Are careful that nobody is looking over their shoulder when they type in a password
- Create a password out of four unrelated words with spaces where possible or a minimum of 9 characters with upper and lower-case letters, at least one number and one special character such as £ or &
- Do not store passwords in plain text on a computer or piece of paper that could be seen by others
- Do not use common password choices such as "password, 12345, p4ssw0rd, pet names, personal name, date of birth, common words such as cities or football teams with letters or numbers replacing vowels such as c0d4, m4nch4st4r un1t4d, f1d0 etc. Note that most password manager applications will generate a unique password for you
- Do not reuse passwords between work and home
- Do not respond to emails asking for their login or asking them to reset a password unless they have requested the password reset themselves 'phishing emails'
- Do not reuse passwords for more than one login
- Never share a password and or attempt to gain access to a system using someone else's username and password
- Report any suspicious emails or activity to the IG lead

Routers and other equipment

The default administrator username and password of our [internet router/firewall/practice computers/other electronic equipment] has been changed.

Encryption

The practice encrypts data whenever possible. Encryption scrambles the data and makes it unreadable unless the user has the encryption key. We use encryption in the following situations:

- Our computers have encryption turned on, in a Mac this is called File Vault, in Windows it is called BitLocker in the Device Encryption section
- iPhones encrypt data by default, we only use Android phones that have encryption, and this is turned on
- Whenever we store personal data on a storage device such as a memory stick, DVD, or external drive the data is encrypted, and the encryption key is kept separate
- Whenever we use a website for business purposes, we check that the browser address bar has a green padlock and says HTTPS instead of HTTP. This means that data sent over the internet is encrypted
- If we need to send a data file by email, either the file is encrypted first, or we use encrypted email (such as ShareFile by Citrix). The encryption key is sent by [post] to the recipient and never by email

Managing logins and levels of computer access

The IG Lead is responsible for who has access to computers and software, as well as the level of access that is appropriate to their role. The Practice Manager is responsible for setting up users when they join the practice, providing the appropriate level of access such as administrator or team member user. The IG Lead is responsible for ensuring that when a team member's role changes, or they leave the organisation, their access to computers and software is appropriately amended or removed.

Wherever possible multi-authentication (MFA) is set up for administrator logins. All logins and their level of access are recorded on the Network, Computer and Software Access Log (M 217L). The IG Lead reviews M 217L [each month] to ensure that team members' access rights are at the right level for their



role.

Audit trail

Each user is allocated a unique username and password, to identify their use of the software. During training each user is given a copy of the guidelines on the use of the system with their login details. A record is kept of all users given access to the software.

New team members

When a new employee/self-employed dentist, hygienist or therapist or external consultant joins the practice, the IG Lead arranges passwords and access level.

Locum staff

Temporary access is granted on a need to use basis by the IG Lead and is recorded in the Network, Computer and Software Access Log (M 217L). Temporary logins are deleted or suspended immediately once they are no longer required.

Change of user requirements

Changes to access level or suspension of an account are made by the IG Lead and a record is kept of all changes on the Computer and Software Access Log (M 217L).

Removal of users

As soon as an individual leaves the practice their logins will be removed by the IG Lead.

Review of computer access rights

The IG Lead reviews all access rights on a regular basis. The review is designed to positively confirm all system users and remove any lapsed or unwanted logons.

Postal services and couriers

To ensure that confidential information transferred from the practice by post or courier is done so as securely as is practicable, the practice ensures:

- Normal post is used for single appointment letters and single referral letters, but for bulk transfers of information, e.g. NHS forms to NHS Dental Services, the practice uses tracked and traced post
- Envelopes are marked "Private and Confidential"
- Packaging is "tamper-evident" (i.e. it is immediately obvious if some-one has attempted access to the contents) and protects the contents from any physical damage likely to arise during transit
- Where necessary, additional controls are applied to protect sensitive information from unauthorised disclosure or modification, e.g. the use of locked containers, locked or access-controlled entry to rooms where post is collected

[Faxes]

The practice's fax machine is in a secure location and when receiving faxes containing confidential information, the practice ensures:

- The fax is removed from the machine on receipt
- Where necessary, the sender is contacted to confirm receipt
- The information in the fax is appropriately dealt with and safely stored, e.g. transferred to the patient record
- Faxes containing patient information are destroyed securely

Additionally, when practice staff members transfer confidential information by fax they always:

- Double check the fax number or use stored frequently used numbers in the fax machine to reduce the risk of typing errors
- Use a fax cover sheet marked "Private and Confidential"
- Send faxes only to a named person rather than a team



- Inform the recipient that a fax will be sent, and ask them to confirm receipt
- Send faxes during an organisation's working hours when staff are present to receive the fax]

Email

Emails received containing patient information are incorporated into the dental record and deleted from the email system on receipt.

The practice is aware that NHS mail is currently the recommended method for sending patient identifiable information by email, therefore the practice ensures:

- Where NHSmail is used to send special category data, this is clearly indicated by the word 'confidential' in the subject header
- Where NHSmail is used to communicate with a non-NHSmail account, it is encrypted by adding the word [secure] in the subject header (including the square brackets)
- When sending special category data by ordinary email it is secured with an encrypted email service [ShareFile/Switch/other] which encrypts any attachments

Transporting

Personal identifiable information is only taken off site when absolutely necessary, in which case the following procedure is followed:

- Record what information you are taking off site and why, and, if applicable, where and to whom you are taking it
- Transport information in a sealed container
- Never leave personal identifiable information unattended
- Ensure that information is returned back on site as soon as possible
- Record that the information has been returned

Other forms of information exchange (e.g. text messages, smartphones, etc.)

Personal identifiable information is always sent by means as described above, with the exception of messages that solely relate to appointment scheduling (such as reminders), which may be sent to a patient's phone or text messaging system if they have previously given permission to use these methods of contact.

The secure use of personal information

When working in an area where patient records may be seen we always:

- Shut / lock doors and cabinets as required
- Query the status of unaccompanied strangers
- Know who to tell if anything suspicious or worrying is noted
- Not tell unauthorised personnel how the security system operates

When using paper patient records, we ensure that they are:

- Only taken out of the practice if absolutely necessary and never removed for general administration purposes, e.g., writing routine reports
- Tracked if transferred out of the practice, with a note made in the tracking register
- Stored and carried in a secure bag/case
- Never left unattended on public transport or in cars (even if they are locked in the boot)
- Kept secure and away from family members and visitors when held overnight in team members' homes
- Returned to the filing location as soon as possible after completion of treatment
- Stored securely within the practice, arranged so that the record can be found easily if needed
- Stored closed when not in use so that contents are not seen accidentally
- Inaccessible to members of the public and not left, even for short periods, where they might be looked at by unauthorised persons



If using electronic records, we:

- Always log-out of any computer system or application when work on it is finished
- Not leave a terminal unattended and logged-in
- Not share logins with other people. If a colleague has a need to access patient records, then appropriate access should be organised for them – this must not be by using your identity
- Not reveal your password to others
- Always clear the screen of a previous patient record before seeing the next patient
- Use a screensaver to prevent casual viewing of confidential information by others

When communicating information about a patient we **take care**:

- Not to discuss patient information in public areas
- If transferring information by phone, or face to face that personal details are not overheard by other people, including staff who do not have a “need to know”
- To anonymise details of the individual being spoken about, especially in high-traffic areas
- Not to leave a confidential message on a patient’s answerphone, as it might be heard by someone other than the intended recipient
- If listening to answer-phone messages that they cannot be overheard by unauthorised persons
- When receiving calls requesting personal information, make sure you verify the identity of the caller (see below) and ask them why they want the information. If in doubt about whether the information can be disclosed, tell the caller you will call them back, and then consult with your manager
- Not to leave messages containing personal information on notice boards that could be accessed by non-authorised staff
- To only discuss a patient’s confidential information with either the patient or their authorised representative. Team members are aware that patient confidentiality even extends to whether a patient is registered to the practice or has arranged an appointment for a particular time
- To obtain written and signed consent from a patient before allowing a family member, or patient representative (e.g. Carer or Personal Assistant (PA)), to book appointments, amend appointments or discuss any matters relating to the patient

When verifying the identity of a caller requesting personal information, we:

- Ask them for their phone number
- Check that it is the correct number for that individual or organisation
- If it is, call them back once you have the decision on whether the information can be disclosed

Transferring patient information

If a team member is authorised to transfer patient information, they follow the information handling procedures.

Handling and retention of criminal record information – DBS/PVG/Access NI disclosures

The IG Lead ensures that information is kept securely in a lockable fire-resistant cabinet with access strictly controlled and limited to persons who need to have access to this information in the course of their duties. This information is only used for the specific purpose it was requested for and with the applicant’s full consent. Note that it is a criminal offence to share criminal record information with any individual who is not entitled to receive it. However, if the applicant freely gives their consent to the sharing of this information, then an offence has not been committed.

The practice does not retain criminal record disclosure details for longer than is necessary; not exceeding six months after the decision has been made to appoint or for six months from the date the applicant was unsuccessful, to allow for the consideration and resolution of any disputes or complaints. DBS, Access NI and PVG Disclosures (M 228) has full details.



Preventing unauthorised computer access

When a desktop computer is left unattended, the team member logs off to prevent unauthorised users' access to it. When leaving a workstation for the day, the team member logs out of the system entirely and closes down the computer.

Audit trails and reporting security breaches

Nearly all of the activity that is performed on a computer can be tracked. Our system suppliers record and enable us to review Internet usage logs. Emails are routinely backed up on the practice's computer servers. Recorded information will be used to aid an investigation where breaches of security, the law or these guidelines, are suspected. This information is kept confidential, but when used helps to explain innocent situations more often than exposing security breaches.

Information security breaches might involve unauthorised use of equipment or unauthorised access to data. Any breach of security, however small, wastes time and often requires work to be repeated and could be a potential risk to the practice or individuals. If you know or suspect that a breach of information security has occurred, please inform your IG Lead.

Using mobile computing equipment

These procedures outline the appropriate use of portable computer devices and removable media, collectively known as mobile computing equipment when it has been purchased or authorised by the practice.

The procedures take into account the increased risk to personal information posed by this way of working and they complement the procedures and guidelines regarding the protection of patient information.

- **Portable computer devices** - includes laptops, notebooks, tablets, and smartphones
- **Removable data storage media** - includes any physical item that can be used to store and/or move information and requires another device to access it. For example, DVD, tape, digital storage device (flash memory cards, USB memory sticks, portable hard drives). Essentially anything that data can be copied, saved or written to which can then be taken away and restored on another computer

NOTE: Team members must **NEVER take patient photographs on a personal smartphone or tablet**. Patient photographs are only taken with a phone or tablet that is owned by the practice and specifically kept for the purpose of patient photography.

Authorisation

Only authorised staff have access to mobile computing equipment. Any member of staff allowing access to any unauthorised person deliberately or inadvertently may be subject to disciplinary action. Staff should **not** use their own (or unauthorised) computing equipment for practice business but they may use a personal mobile phone for the iComply mobile application.

Be aware of security measures in place

To reduce the risk of loss and unauthorised access we have the following measures:

- Mobile Equipment Terms and Conditions (M 217I) are completed for each mobile computing device provided to a staff member and this person is listed in the Mobile Equipment Log (M 217H) as the nominated responsible owner
- Encryption is applied to all mobile computing equipment
- Password protection is setup on laptops and smart phones [and where available Face ID or Fingerprint ID]
- Everyone with portable equipment must update anti-virus software weekly and run a scan
- Regular backups are taken of the data stored on the mobile equipment
- Issue and return of mobile computing equipment is recorded in the Mobile Equipment Log (M 217H) ensuring that the device's serial number or International Mobile Equipment Identity (IMEI)



number is recorded so that it can be given to the phone/device operator in the event it is lost or stolen

- All devices have been registered with the UK National Property Register, which assists the police in reuniting owners with their stolen property
- [Find my iPhone, Windows Find My Device, Blackberry Protect, Android Device Manager etc] has been installed on all mobile equipment to ensure that the data on the device can be quickly erased if it goes missing
- Our IT company has installed Mobile Device Management (MDM) which allows for remote deletion of data

Team members:

- Store mobile equipment securely when not in use on and off site, never leave visible in a car
- Ensure files containing personal or confidential data are adequately protected e.g. encrypted and password protected
- Virus check all removable media e.g. USB drives, portable hard drives, etc. prior to use
- Obtain authorisation before you remove mobile equipment from the premises
- Be aware that software, Intellectual Property and any data files created by you on practice mobile equipment are the property of the practice
- Report **immediately** any stolen mobile equipment to the IG Lead. Failure to report a stolen mobile phone could result in significant charges from the phone company
- Be aware that the security of your mobile computer equipment is **your** responsibility
- Ensure that mobile equipment is returned to the practice if you are leaving. Note that a final salary deduction may be made if equipment is not returned

Team members do not:

- Disable the virus protection software or bypass any other security measures put in place
- Store patient information on mobile equipment unless the equipment is protected with encryption, and it is absolutely necessary to do so
- Take personal data or special category data out of the practice without authorisation, this includes clinical records
- Use the practice's mobile computer equipment outside the practice premises without authorisation
- Use a personal mobile computer equipment for practice business [apart using the iComply mobile application on their own phone]
- Allow unauthorised personnel/friends/relatives to use mobile equipment in their charge
- Use public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (where no password is required to access it)
- Leave mobile equipment in places where anyone can easily steal them
- Leave mobile equipment visible in the car when travelling between locations
- Leave mobile equipment in an unattended car
- Leave mobile equipment unattended in a public place e.g. hotel rooms, train luggage racks
- Install unauthorised software or download software/data from the Internet
- Delay in reporting lost or stolen equipment

Personal use of practice email, internet and phones – policy and procedure

We permit the incidental use of internet, and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must be neither abused nor overused and we reserve the right to withdraw our permission at any time. The following conditions must be met for personal usage to continue:

- Use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 5.30 pm)
- Personal emails must be labelled "personal" in the subject header
- [You must never use webmail such as google mail as this could bypass the practice anti-virus



system]

- Use must not interfere with the team member's practice commitments
- Use must not commit the practice to any marginal costs
- Use must comply with practice policies including the Anti-bullying and Harassment Policy (M 233-ABH), Equality, Dignity and Human Rights Policy (M 233-EQD), Data Protection and Information Security Policy (M 233-DPT) and the Social Media Policy (M 233-SMD)

Team members should be aware that personal use of our systems may be monitored and, where breaches of this policy are found, action may be taken under the disciplinary procedure. We reserve the right to restrict or prevent access to certain telephone numbers or internet sites if we consider personal use to be excessive. In general, team members should not:

- Send or forward private emails at work which they would not want a third party to read
- Send or forward chain mail, junk mail, cartoons, jokes or gossip
- Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to those who do not have a real need to receive them
- Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals
- Agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter
- Download or email text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this
- Send messages from another worker's computer or under an assumed name unless specifically authorised or
- Send confidential messages via email or the internet, or by other means of external communication which are known not to be secure
- Keep an email which has been sent to the wrong address in error, it should be returned to the sender

Misuse or excessive use or abuse of our telephone or email system, or inappropriate use of the internet in breach of this policy will be dealt with under our Disciplinary Procedure. Misuse of the internet can, in certain circumstances, constitute a criminal offence. In particular, misuse of the email system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will amount to gross misconduct (this list is not exhaustive):

- Pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature)
- Offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our patients
- A false and defamatory statement about any person or organisation
- Material which is discriminatory, offensive, derogatory or may cause embarrassment to others;
- Confidential information about us or any of our team members or patients (which you do not have authority to access)
- Any other statement which is likely to create any liability (whether criminal or civil, and whether for you or us) or
- Material in breach of copyright

Any such action will be treated very seriously and is likely to result in summary dismissal. Where evidence of misuse is found we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.



Personal mobile telephones

Personal mobiles should be turned off during working hours. Messages will be taken for team members during working hours, but they would not be expected to come to the telephone unless there was an emergency. Personal calls should never be made from reception or in the treatment room if patients could overhear the conversation.

Using personal devices for work purposes (“Bring your own device”)

This practice allows team members to use their own devices for certain limited work purpose. The practice of allowing employees to utilise personally owned devices is known as “Bring your own device” or “BYOD”.

BYOD is offered at the practice’s discretion and may not be available to all team members. This practice reserves the right to revoke access if staff do not follow this policy.

The purposes for which a team member may use their own device for work purposes are limited to:

- Accessing [Agilio iTeam] to manage sickness, absence, holidays and their key HR documents
- Accessing [Agilio iComply] to manage practice compliance tasks
- [Other]

Team members must:

- Only connect to organisation systems for the purpose of authorised work
- Keep their passwords secure
- Use biometric features to secure the device if possible
- Keep their operating system updated
- Be careful who can see their screen when accessing work systems
- Report lost or stolen devices
- Facilitate the practice to conduct spot checks if required

Team members must not:

- Share their device or passwords
- Make copies of data or take screenshots
- Access systems without authorisation
- Save work in unapproved locations or applications

Team members are solely responsible for all costs associated with purchasing, running, repairing and replacing their personal devices used with BYOD. Team members are responsible for all mobile data or Wi-Fi hotspot costs related to BYOD usage and should monitor these to ensure they have sufficient allowance.

How is this BYOD enforced?

The practice will monitor usage of BYOD devices from time to time including the make and model of devices in use and the version of the operating system currently installed. Where operating systems are found to be out of date the team member will be informed and expected to upgrade to the most current version within five days. Failure to remediate will result in access to BYOD services being withdrawn.

Spot checks on BYOD devices may be initiated at any time and team members will be expected to allow access to by the practice manager to check settings related to BYOD usage. Spot checks will always be conducted in the presence of the team member and devices will never be taken away from their owner.

This practice will undertake spot checks at least every twelve months. The IG Lead will create a task in iComply to record these checks and notes any follow-up actions required.

Technical support personnel may access details on usage of corporate applications via the BYOD system



but cannot access personal application data. In some instances, device location may be collected but this data will only be used if the device is lost or stolen.

Lost or Stolen Devices

When a team member notifies the practice that their device has been either lost or stolen, steps should be taken immediately to block the team member's account(s) and reset any passwords/access codes on the work systems that were installed on their device. This will help to prevent any unauthorised access. Team members should also be encouraged to use security services available to them on their device such as find my iPhone or Android Device Manager etc.

Data and Cyber Security Tests

[If you are an NHS provider or have an NHSmail account - To comply with the DSP Toolkit we must demonstrate how we test our contingency measures data and cyber security breaches. To do this, we annually review the cyber and security aspects of our Disaster Planning and Emergency Procedures (M 255). We log details and the outcomes of these tests in Data and Cyber Security Test Log (M 217X).]

Managing Data Breaches

Notification requirements

Where relevant this document is read in conjunction with the Disaster Planning and Emergency Procedures (M 255). The IG Lead is responsible for managing data breaches. This data breach management applies 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 e.g. unauthorised access, data loss or theft causing an actual or potential breach of confidentiality
- Integrity, e.g. records have been altered without authorisation and are therefore no longer a reliable source of information
- Availability, e.g. records are missing, misfiled, or have been stolen

When a data breach is reported to the practice

It could be reported by an affected patient, by a relative, a member of the public or by a team member, the IG Lead will:

- Interview the complainant to establish the reason for the complaint and why the practice is being considered responsible
- Complete the [Event Record and Register/iComply Digital Event Record]
- Investigate according to the information given by the complainant
- Record findings, e.g. unsubstantiated concern, suspected/potential breach, actual breach, etc.
- Where necessary, provide written explanation to the patient with formal apology if warranted
- 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, notification to the authorities etc.

When an Event happens – if it needs recording it is probably a Significant Event and needs Significant Event Analysis (SEA) to determine what went wrong and how to stop it happening again – then you will decide if it is a Safety Incident, Serious Incident or equivalent.

Any actual or potential information incident in the practice will be investigated and managed accordingly. In all cases the IG Lead will complete [an Event Record (G 110A) and log the record on the Events Register (G 110B)/the iComply Digital Event Record].

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. The confidential material could be on paper, hard drive, computer or storage media such as memory card or stick or tapes, etc. If it happens the IG Lead



will:

- Investigate how the information left the practice by interviewing staff and contractors as appropriate
- 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
- Consider whether the patient(s) should be informed and where it is judged necessary, provide a written explanation to the patient(s) with a formal apology
- Record findings, e.g. potential breach, actual breach, evidence of misuse, etc.
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, notification to the authorities etc.

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, the IG Lead will:

- Check the Information Asset Log (M 217G) to find out whether equipment is missing
- Investigate whether there has been a legitimate reason for removal of the equipment (such as repair or working away from the usual base)
- If the cause is theft, inform the police, ask them to investigate and keep them updated with your findings
- Interview staff and check the Information Asset Log (M 217G) to establish what data was being held and how sensitive it is
- If possible, establish the reason for the theft/unauthorised access, such as:
 - Sale of items
 - Access to material to embarrass the practice
 - Access to material to threaten patients (blackmail, stigmatisation)
- Consider whether there is a future threat to security
- Inform insurers
- Review the physical security of the practice
- If there has been unauthorised access to the practice computer system:
 - Ask the system supplier to conduct an audit to determine whether unauthorised changes have been made to patient records
 - Consider whether any care has been provided to patients whose records have been tampered with
 - Check compliance with access control procedures, e.g. ensure passwords haven't been written down, staff members are properly logging out, etc.
- 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)
- If computer hardware or the core software has been stolen, inform system suppliers to enable restoration of system data to new equipment
- Record findings, e.g. potential breach, actual breach, evidence of tampering, compromised or delayed patient care, etc.
- Take and document appropriate action, e.g. physical security improvements, advice/training, disciplinary measures, notification to the authorities etc.

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. The IG Lead will:

- Interview the person reporting the incident to establish the cause for concern
- Establish the facts by:

- Asking the system supplier to conduct an audit of the activities of the user concerned
- Interview the user concerned
- Establish whether there is a justified reason for the alleged computer misuse
- 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
- Record findings, e.g. breach of confidentiality, evidence of tampering, fraud, carrying on a business, accessing pornography, etc.
- Take and document appropriate action, e.g. no action as allegation unfounded, training/advice, disciplinary measures, notification to the authorities etc.

Lost or misfiled paper dental records

This type of incident could have a possibly severe impact on patient care as the information within a patient record is incorrect or is not available when required. The IG Lead will:

- Investigate who last used/had the paper record by interviewing staff and contractors as appropriate
- Consider whether any care has been provided based on incorrect information within a patient record
- Consider whether patient care has been delayed due to information not being available
- Establish whether missing information can be reconstituted, e.g. from electronic records
- If information within records has been misfiled, ensure it is restored to correct filing order/ returned to the correct record
- Where necessary, (i.e. if care affected) provide a written explanation to the patient with a formal apology
- Record findings, e.g. compromised or delayed patient care, etc.
- Take and document appropriate action, e.g. advice/training, disciplinary or contractual measures, notification to the authorities etc.

If a team member discovers a data breach?

If a team member discovers something that could be considered a data breach it is reported to the IG Lead, an [Event Record (G 110A) is completed and it is entered on the Event Register/and the iComply Digital Event Record is completed]. The following information is entered on the form:

- The team member's name
- The date the incident was discovered
- Where the incident occurred
- Details of the incident
- The decision of the IG Lead as to whether it is reportable or not
- Any initial actions that were taken - including who the incident has been or will be reported to and the date the report is made
- Any other information including patient or other correspondence

Notifiable breaches will be reported to the ICO and the Local Area Team within 72 hours following the Notification Requirements above. If necessary the patient/s involved will be informed by letter without delay, advising them of the details of the breach and any actions that they need to take. Patient concerns and feedback will be handled by the IG Lead.

Data breach notification procedure

The 'Notification Requirements' are at the beginning of this section.

In England NHS dental practices must use the online Data Protection and Security Incident Reporting Tool Direction 2018. This will report it to the Information Commissioner's Office, the Department of Health and Social Care and the National Cyber Security Centre.



All practices in Wales and fully private practices in England should submit a report to the Information Commissioners office using the ICO [Security breach notification form](#). All practices must keep a record of all personal data breaches and record the basic facts, effects of the breach and remedial action.

Lessons learned from a data breach

The practice maintains a register of all incidents occurring (a Significant Event) by [creating an Event Record (G 110A) and making a note of it on the Event Register (G 110B)/completing the iComply Digital Event Record].

Significant Events and Serious Incidents are discussed at a practice meeting to provide staff with an example of what could occur, how to respond to such events and how to avoid them from happening in the future. If necessary, an Ad-Hoc Audit is carried out (the Ad Hoc Audit template is in iComply).

Remote access policy and procedure

Remote access to the practice is necessary for people who do not work from the premises at all times. Authorised users are called hosts, they need to log onto our network using a Virtual Private Network (VPN). To protect confidential personal data, it is necessary to have the highest standards of security. The purpose of this procedure is to minimise:

- Accidental, unauthorised or inappropriate access to electronic data
- The chance that the practice network could be compromised
- Damage to the integrity, availability and confidentiality of the practice network and IT system
- The possibility of damage to the practice reputation through loss or misuse of data

Here are the rules for using remote VPN access:

- The practice uses [VPN name e.g. Open VPN with <https://www.privatetunnel.com>] to allow hosts to connect remotely
- The practice network has a [name of firewall] firewall
- Host logins are recorded in the Network, Computer and Software Access Log (M 217L)
- Hosts must follow the password rules in this procedure (M 217C)
- Any IT equipment used to connect using VPN must have the latest software updates, anti-virus software and definitions and weekly virus scans
- Any IT equipment provided by the practice is for the host's use only
- Hosts must protect their username and login, even from family members
- A host can only connect to the practice VPN using [the computer/laptop supplied by the practice]
- Any patients' or team members' personal data viewed away from the practice must be kept completely confidential and steps taken to ensure that it is not seen by anyone else, special care must be taken in public areas
- A breach of this policy and procedure may lead to disciplinary action
- The practice may monitor the use of a host's VPN to verify compliance with these rules

Staff confidentiality code of conduct

The practice has produced this Staff Confidentiality Code of Conduct to raise staff members' awareness of their legal duty to maintain confidentiality, to protect personal information and to provide guidance on disclosure obligations.

Personal information is data about patients or staff, 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 such as race, health, sexuality, bank account details etc. This code also covers information about deceased patients.

Recognise your obligations

A duty of confidence arises out of the common law duty of confidence, employment contracts and your



professional obligation as a registered dental professional. 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, you must 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

Keep personal information private

To keep personal information protected make sure you observe the practice policies and procedures listed in the Data Protection and Information Security Policy (M 233-DPT).

Disclose with appropriate care

It is the aim of the practice to ensure that patients are adequately informed about the use and disclosure of their personal information. Refer to Patient Leaflet on Personal Information (M 217P). You should be familiar with it and seek advice from the IG Lead if you are unable to answer patients' questions.

If you are authorised to disclose personal information you should ensure you do so in accordance with 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 IG Lead who will consult the medical indemnity provider before releasing the information.

Information disclosure over the phone

Before information can be disclosed a staff member should:

- Confirm the name, job title, department and organisation of the person requesting the information and the reason for the request if appropriate
- Take a contact telephone number (e.g. main switchboard number, NOT a direct line or mobile)
- Check whether the information can be provided. If in doubt tell the enquirer you will call back
- Provide the information only to the person who has requested it (do not leave messages)
- Record your name, date and the time of disclosure, the reason for it and who authorised it, details about the medical indemnifier who agreed you could provide it. Record the recipient's name, job title, organisation and telephone number

[England only: Data Opt Out



Our practice only uses your personal health data to provide individualised care to you and does not disclose your data for any other purposes. The national data opt-out does not apply to our usage of your data and we are compliant with the policy.

Our practice takes part in [research projects] where the opt-out could apply. We are compliant with the national data opt-out policy.]

Data security incident response and management plan

The data breach management plan is in this document and the disaster recovery plan for data and practice computers is in Disaster Planning and Emergency Procedures (M 255).

