Woodbrook Medical Centre

Communication Policy

Version:	Review date:	Edited by:	Approved by:	Comments:
1	2 February 2022	NB		
1.1	November 2024	Anne Jones	Anne Jones	Uploaded latest version of policy as many changes to Policy including AI

Table of contents

1 Introduction

1.1 Policy statement

This document has been produced to provide all staff at Woodbrook Medical Centre with the necessary information to ensure that they understand how communication works internally and externally and how they are involved in the communication process. Excellent communication is essential to deliver a service that meets the needs of those who use the organisation's services.

This policy will explain how communication works within and outside the organisation and the responsibilities of all staff members. Furthermore, it explains the different means to communicate and the nuances that are required to effectively manage these.

1.2 Status

The organisation aims to design and implement policies and procedures that meet the diverse needs of our service and workforce, ensuring that none are placed at a disadvantage over others, in accordance with the Equality Act 2010. Consideration has been given to the impact this policy might have regarding individual protected characteristics of those to whom it applies.

This document and any procedures contained within it are non-contractual and may be modified or withdrawn at any time. For the avoidance of doubt, it does not form part of your contract of employment. Furthermore, this document applies to all employees of the organisation and other individuals performing functions in relation to the organisation such as agency workers, locums and contractors.

2 Communication considerations

2.1 General

Understanding and respecting patient preferences means that patients need to be aware of the range of communication options available to them, to be informed of the potential risks of each communication format and to indicate their preferences against each.

Since 2016, all organisations that provide NHS care and/or publicly funded adult social care are legally required to follow the Accessible Information Standard. Further reading can be sought in the Accessible Information Standards Policy.

There will be occasions when patients will require the services of an interpreter and/or a translator. For detailed supporting guidance, refer to the Translator and Interpreter Policy.

2.2 Significance of communication

Communication may be between clinicians, clinician and patient, clinician and non-clinical staff, non-clinical staff and patient. The several means of communication which are discussed throughout this policy.

All staff must be effective communicators as they play a key role in the provision of information to patients, carers, colleagues and external stakeholders. It is therefore pivotal that information is relayed in the most appropriate and timely manner to ensure the safe and effective care of patients and to enable the organisation to function efficiently and effectively.

The identification of patient contacts is vital and, as such, a telephone caller's identity and credentials must be verified, ensuring that they are the patient or that they have the consent of the person they are calling about. It is also important that, as a principle, when there is communication related to patient care, an appropriate note is recorded in their clinical record by clinicians and non-clinicians alike.

2.3 Monitoring frequency

For communication to be effective, messages must be processed in an acceptable time frame. It is considered best practice for staff to check all messaging systems such as email, messenger, clinical systems, text messages, etc. at least three times daily, usually at the start of the working day, around midday and late afternoon before the organisation closes.

In the following chapters, detailed guidance is provided on each different communication method.

3 Emails and SMS

3.1 Email use

All staff will be given an NHS email address upon joining which is for the use of practice business only. NHS emails should not be used for personal use, nor should the content of any email bring this organisation into disrepute.

Emails should be written in a clear and concise manner and should be relevant to the subject heading. The organisation will establish a standard signature block and disclaimer regarding use of information contained in the email.

3.2 Contacting patients by email or SMS

Patients may actively and consistently use email or SMS text messaging as their preferred method of communication. Therefore, is imperative that the patient confirms both email address and mobile telephone number to enable this organisation to verify the accuracy of the information held. While it is the responsibility of the patient to ensure that they provide up to date contact details, we will often confirm these details when either in attendance or when contacting the practice.

Patients will be reminded that the organisation is not responsible for the protection of the information once it has been received by the patient. It is also to be recommended to the patient that they do not use a shared email address for the purpose of communicating so that confidential information will not be seen by family members. Furthermore, and specific to emails, patients are to be advised that internet email accounts are not secure and that there is a risk of their email being hacked.

This organisation will not accept any responsibility for the loss of confidential information should a patient's email account be hacked.

3.3 Email parameters

Only appropriate matters will be dealt with using email. The clinical lead has agreed to the following being acceptable:

- Appointments
- Repeat prescription queries
- Requesting test results
- Requesting copies of medical records
- Emails containing images of a clinical condition

Requests for complex information about medical conditions or symptoms are not appropriate for email communication. Instead, the organisation will telephone the patient to ask them to make an appointment to discuss the matter with an appropriate member of the clinical team.

Additional information can be found in NHS Digital Guidance for sending secure email (including to patients) and also the Audio Visual and Photography Policy including the medico-legal expectations for receiving any intimate images.

For further guidance refer to:

- Access to Medical Records Policy
- Managing Incoming Pathology Results
- CQC GP mythbuster 46: Managing test results and clinical correspondence

3.4 Out of office function

Staff members who are often required to either send or receive emails are to ensure that they utilise the "out of office" function detailing the period of leave. An alternative contact can be added to the message.

3.5 Consent for patient communication via email or text

As consent is not used as a legal basis for data processing, messages are therefore sent on an 'opt-out' basis. If a patient informs this organisation that they do not wish to receive text messages, a member of staff must update their 'notification preferences' in the clinical system.

When a patient provides either a mobile phone number or email address, the NHS E document titled Email and text message communications deems this to be sufficient consent to then send them either an email or a SMS text message. However, this is provided that a Data Protection Impact Assessment (DPIA) has been undertaken and that all reasonable steps have been made to ensure the communication methods used are both secure and are meeting their transparency responsibilities.

NHS E is supportive of text messaging in the delivery of care and remind practices of the need to ensure that they inform patients as to how they may be contacted and what they may be contacted for, such as:

- Appointment reminders
- Appointment letters
- Individual invitations to screening, medication reviews, vaccination appointments

- Test result notifications/advice to call the practice where action is needed
- Friends and family test surveys
- Interactive messages with the ability to confirm/cancel appointments

In addition, this organisation allows patients to contact them via email and text message for the following:

- Ordering repeat prescriptions via email/online message
- Requesting appointments or non-urgent advice
- Updating them on your health and care

It should be noted that this NHS E advice does contradict the current, albeit older, advice from both the MDU and the MPS as detailed in the following documents:

- MDU - Text message communication in general practice
- MDU - Avoiding email dangers
- Medical Protection Society - Communicating with patients by test message

Under the Data Protection Act 2018 (DPA18) and the UK General Data protection Regulation (GDPR), re-consent does not need to be considered for those patients already receiving text messaging services. For more information on consent, refer to the Consent Guidance.

3.6 Compliance actions

This organisation will meet its transparency responsibilities by providing information about how it uses email addresses and mobile telephone numbers. This will be promoted via the following means:

- During registration via the New Patient Registration and Health Check Policy
- When a mobile phone or email address is recorded/confirmed or updated
- The Practice Privacy Notice that is available on the practice website
- Within posters that are placed in patient areas such as:
  - Email and text messaging poster
  - Text messaging service poster

Should a patient have a preference or wish to opt out of any communications, they can complete the form at Annex A and as detailed at Section 3.11. Should proxy action be required, then the proxy access preferences form is to be completed at Annex B and as detailed at Section 3.15.

3.7 Ensuring information is correct

Patient circumstances can change over time and these preferences should be actively maintained. The fourth Data Protection Principle adopted into UK law states that all personal data processed shall be accurate and, where necessary, kept up to date. This is commonly referred to as the accuracy principle.

When text message communication is intended to be used for test results, it is recommended that the patient's preference is checked during each contact.

3.8 Data Protection Impact Assessment (DPIA)

To support the rationale to offer service users a text or email option, a DPIA will be undertaken. This DPIA will include all aspects of the process including retaining any information and ensure that all methods of communication used are secure.

A DPIA template can be found within the UK GDPR Policy.

3.9 Generic email address

This organisation will only communicate with patients from generic email addresses as this provides reassurance to patients that the email they have received is legitimate. Ordinarily staff should not communicate with patients from their individual @nhs.net email account.

This organisation will ensure it sends an automated response indicating that the email has been received.

3.10 Email retention

Emails are classed as records and are to be added to the patient's healthcare record and have the appropriate SNOMED CT code included. Staff are to add a short summary of the email to the record, for example:

- "Patient emailed regarding test results; replied with results and advised patient to book an appointment with the Practice Nurse"

- "Patient emailed requesting information about symptoms they are experiencing. Advised patient to book an appointment as it is not appropriate to discuss this using email. Patient has subsequently booked an appointment"

Should any patient email contain relevant information, including image(s) regarding their ongoing clinical condition, at the clinician's discretion, this is to be uploaded to the patient's medical record.

To meet with the rulings of the Data Protection Act 2018, once uploaded to the clinical record there no longer remains any need to retain the email. It is the responsibility of any recipient of the email to delete the message once the action is complete.

This information should be shared with patients within the practice leaflet and upon the website.

3.11 Opting in or out of communication via email or text

For the method of being contacted, patients may request to opt-out of receiving either SMS text messages or emails. In some instances, patients may wish to only receive specific types of information. An example is when a patient prefers to receive a text appointment reminder but does not wish to be sent test results.

The form that details a patient's wishes for being contacted by either email, text or both is at Annex A. Note that this does not need to be completed for all patients who provide their email address or mobile telephone contact number as this is then considered to be implied consent and as detailed at Section 3.3.

Should a patient wish to fully or partially opt-out, then this organisation will use alternative methods of communication. All decisions will be detailed within their clinical record to ensure that all staff know of their preference.

The following SNOMED CT codes will be used:

SNOMED code	Title
705025004	Consent given for communication by email
835231000000104	Declined consent for communication by email
699237001	Consent given for communication by SMS messaging
911361000000104	Consent given to receive test results by SMS messaging
513631000000106	Declined consent for communication by SMS messaging
911401000000108	Declined consent to receive test results by SMS messaging

Patients should be free to update and change their preferences at any time and expect those changes to be effective immediately.

Further reading on both email and text messaging requirements and best practice can be found in the NHS E Template for email and text message communications
and Gov.uk Screening text message principles.

3.12 Sending SMS messages and etiquette

Convenience allows patients to receive SMS text messages that contain non-sensitive information as part of the routine advice or reminder service. Staff must refrain from using abbreviations or 'text speak' and ensure that messages are written in a language that is understandable and unambiguous.

Each message should include the following as the final line: "This text-messaging service is unable to receive replies. For all enquires, contact the practice on XXX". Under no circumstances are any staff to use their personal mobile phones to send messages to patients.

When sending a text message to a patient, staff members must consider the 4c's, that being:

- Consent
- Confidentiality
- Child/age of the recipient
- Content

Emails and text messages should not be sent to patients before 08.30 or after 20.30 unless it is felt appropriate to do so, for example a patient is awaiting an urgent prescription before their holiday.

3.13 Text message content

While this method of communication is time-efficient, improves communication and is particularly beneficial to patients with impaired hearing, the potential to breach patient confidentiality must also be a consideration.

SMS text messages should not contain sensitive information. Sensitivity is not determined solely by the type of information (clinic appointment) but requires a judgement as to the impact if the information was misused. Some information is especially sensitive, such as issues relating to sexual health and mental health.
Texts can efficiently be sent to patients to convey the following information:

- Reminder of their forthcoming appointment at the organisation
- The need to call the organisation to arrange an appointment
- A new patient health check is due
- The need to call the organisation to rearrange an appointment due to the cancellation of a clinic
- Log on details for video conference consultation

There is no way of guaranteeing that a message has been read by the intended recipient, therefore:

- Messages containing critical information should not be relied upon (e.g., abnormal blood test results requiring immediate action) unless they are followed up to ensure the information was received
- If the patient's mobile phone number has been verified, the delivery receipt can confirm that the message has arrived on their phone.

Without consent, staff should avoid sending sensitive information as SMS messages can be overseen and therefore may be viewed by a patient's relative, friend or colleague.

Messages should be phrased professionally but do not require the same level of formality as a letter. Text abbreviations, e.g., 'thnx', 'u', are not appropriate.
When using a template, for guidance, examples are:

Appropriate message	Inappropriate message
Administrative information, e.g., prescription ready to collect	Worrying, complex or sensitive test results, e.g., STI test or high PSA
Care plan sent in a consultation, e.g., dosage of new medication	Long or complex messages, e.g., multiple medication changes
Recall, e.g., advising the patient to book an appointment	Links to sensitive patient advice without consent, e.g., family planning advice
Advice and safety netting sent in a consultation, e.g., link to NHS website information or MSK exercise videos	Signposting to third-party services without consent, e.g., Macmillan contact details

Signposting to third-party services in a consultation, e.g., exercise classes	Critical information without follow-up, e.g., urgent appointment required
Normal test results, e.g., chest x-ray normal	
Some abnormal results, e.g., low vitamin D with advice for sun exposure and OTC supplements	
Telephone information, e.g., you tried to call but could not reach them, or will be calling	
Reminders, e.g., for cervical screening or overdue blood tests	
Follow-up, e.g., checking a patient has received a hospital letter after a referral	

All SMS messages are recorded within patients' healthcare records.

3.14 Delivery reports

Staff can see when a message was delivered to a patient, or if the delivery failed, by reviewing 'delivery reports'.

If an SMS text message is shown as undelivered, a further attempt will be made to send the same message again. If this is again unsuccessful, then either a telephone call will be made or a letter will be sent with the same content as used in the text message and the failure should be coded into the patient's notes using the appropriate SNOMED CT code:

864231000000108	Failed encounter – short message service text message delivery failure

3.15 Proxy access

Consent would need to be obtained to forward an email to a carer, relative, responsible adult or partner. Proxy access may be given to both email and/or SMS text messaging services. Proxy access can be requested via the consent for proxy access to email or SMS form at Annex B.

Should the practice opt not to grant the person access to the text messaging service, the Practice Manager will contact the patient and advise them of the reasons why this decision has been reached.

3.16 Children and young people's access

Children and young people may be keener for interaction via text message as this is more commonplace as their means to communicate. However, with this comes greater challenges as, while children and young people may refer to use SMS regarding their care, particular attention should be given to:

- Highlighting the ability for children and young persons to request that their contact details are used instead of their parents or carers

- Having the correct contact details

- What information is to be sent to them for specific episodes of care as their healthcare record may contain alternative contact numbers for both them and their parents or carers

- Children and young people may wish general care information to remain communicated to their parents, e.g., check-ups, service information etc., while wishing for a particular test result to be texted only to them

- It should not be presumed to automatically include parents or carers in any communication

It is difficult to say at what age the child will become competent to make autonomous decisions regarding their healthcare as, between the ages of 11-16, this varies from person to person.

In accordance with Article 8 of UK GDPR and Part 2, Chapter 2, paragraph 9 of the DPA 2018, from the age of 13, young people are able to provide their own consent and will be able to register for text messaging services.

People aged 16 or above are assumed to be competent to make an independent and informed decision about whether to ask for someone to have proxy access to their text messaging service unless there is an indication that they are not. Care must be taken to determine who has parental rights for a child under 11 or a patient over 16 who is not competent to control access. Care must also be taken if a parent has no, or limited, legal right of access because they have been perpetrators of abuse and/or neglect.

The approach as detailed within the RCGP document titled GP Online Service Guidance: Children and Young People is to be adopted. Further reading can be found in CQC GP mythbuster 8: Gillick competency and Fraser guidelines.

A flowchart to support the access process is available at Annex C.

3.17 Continuous improvement

To fully embed text messaging as a way of working and maximise the benefits for the organisation, staff and patients, the lead who is responsible for improvement initiatives should encourage the use of SMS by:

- Presenting usage across the team by discussing at practice meetings. Those staff who regularly use SMS as a form of communication should share the benefits

- Gathering patient feedback on the service and identifying other opportunities to provide a better patient experience using text messaging. Discuss any findings and opportunities with the patient participation group (PPG)

- Developing a library of practice text templates and relating these to other practice protocols (e.g., care navigation, test results, self-care). Share these with other practices to obtain their considerations

- Completing audits to ascertain patients' needs. This could also include types of messages sent and whether SMS is the best form of communication as the patient may have a poor signal reception

3.18 Receiving text messages

Should the organisation have a mobile telephone as an alternative method of communicating and should patients be able to send messages to this number, the administration team are responsible for ensuring that these messages are read and any appropriate action has been completed.

Details of this service are available within the practice leaflet and website along with guarantees as to how this organisation manages patient data that is forwarded by text message citing the privacy notice

To ensure that data protection considerations are met, the message, including any image, will be deleted once it has been uploaded to the patient's clinical record although, in accordance with Article 35 of UK GDPR as detailed at Section 3.7, a DPIA will also be undertaken to reflect this method of receiving and maintaining patient data.

For further information, refer to the UK GDPR Policy and the Practice Privacy Notice.

4 Website and practice leaflet

4.1 Website

It is a contractual requirement to include the detail as listed within Part 4 of NHS E document Creating a highly useable and accessible GP website.

Note that any information on how to access GP services should remain correct and up-to-date.

4.2 Practice leaflet

The information within the practice leaflet must also reflect that which has been added to the website. Further information is detailed within the above link to Part 4 of the NHS E document.

Supporting documents can be found in the following:

- Practice Information Leaflet Guidance
- Practice Information Leaflet template
- Children's Privacy Information Leaflet template

The Practice Manager is to be appraised of any out-of-date or incorrect information that is found on either the practice website or leaflet.

5 Internet use

5.1 Principles of acceptable use

All staff will have access to the internet, shared network drives and the intranet to enable them to perform their duties. The use of the internet facility by staff is permitted; however, it is only authorised during official breaks or when it is necessary to complete a specific task or when approved by line managers.

Staff are reminded not permitted to use the internet for any of the following purposes:

- Pornography
- Gambling
- Promotion of terrorism and/or terrorism skills
- Cult-promoting websites
- Any other website that may reasonably bring the organisation into disrepute, such as those that are likely to cause offence

To support this, remote access from CSU, the Information Governance Lead or Practice Manager all have the right to scrutinise the internet browsing history of staff members and, if it is found that staff are using the organisation's IT facilities for such activities, disciplinary action will be taken. This may include involving the local police depending on the nature and source of the information.

6 Social media

6.1 General

Social media is a useful method to quickly disseminate information such as early closure, advertising specific clinic dates or to advertise health promotions campaigns or initiatives. However, all content that is posted onto any of the organisation's social media pages is restricted to ensure that only appropriate comments or pictures are uploaded.

6.2 Acceptable use

Work-related issues must not be placed on any social networking site at any time as this could identify an individual and breach patient or employee confidentiality. Work content or material or contacts or connections list created by an employee during their employment on any of their authorised social networking sites shall remain the property of the organisation.

Upon termination of employment, any employee who is a social media administrator shall hand over access rights to their accounts together with any work content or material and any contacts or connections lists.

Furthermore, additional reading can be sought in:

- Patient Social Media and Acceptable Use Policy
- Confidentiality and Data Protection Handbook
- Caldicott and Confidentiality Policy

6.3 Social media platforms

Only information that has been approved by the nominated individual may be posted on the organisation's social media platforms. Staff are not permitted to use the organisation's social media platforms to make any unrelated posts. To prevent inappropriate usage of the platform(s), access is limited to the nominated individuals.

The monitoring of the platform(s) for comments and feedback from patients is the responsibility of the management team. The specific requirements are outlined in the individual's Terms of Reference.

6.4 Inappropriate staff use of personal social media accounts

It is not the intention at this organisation to interact with the personal lives of staff. However, it may be considered a disciplinary offence, up to and including gross misconduct in accordance with the Disciplinary Policy and Procedure, should any staff member post an article or image upon their personal social media account that is subsequently deemed to compromise either:

- Their professional standing
- The organisation
- Another staff member
- A patient

Prior approval must be sought from the Practice Manager for any image that has been taken of any event, such as a flu clinic, to be uploaded to a personal social media account for public viewing.

The Practice Manager will review any image to ensure that it is appropriate and that the organisation is always seen favourably.

6.5 Sharing images of staff members

When an image that identifies another staff member(s) is taken, the staff member captured in the image is to be asked for their consent prior to this being uploaded to any social media account.

Failure to do so may be a breach of the staff member's human right to enjoy the right to privacy. This includes whether the image is taken within the organisation or externally such as an organised social function.

It should be noted that particular care must be taken when capturing any image from within the workplace as this may inadvertently breach patient confidentiality. Should this occur, this may be considered as per the Disciplinary Policy and Procedure.

Further guidance is detailed in the Caldicott and Confidentiality Policy.

6.6 Instant messaging

While most staff members will have access to emails and instant messaging (IM) such as WhatsApp, unless specifically stated within the contract of employment, the joining of any organisational IM group is voluntary and not an expectation.

IM is an effective tool, particularly for communication and the rapid sharing of information, it also provides end-to-end encryption (AES 256) and as such, offers users a secure means to share information.

At this organisation, IM groups have been created to expedite the sharing of information, although staff must ensure that when they use IMs, they:

- Do not include any patient identifiable information
- Acknowledge that any IM messaging conversations may be subject to freedom of information or subject access requests
- Do not use an IM in lieu of the medical record

Staff must ensure the following security measures are put in place:

- Set up a device passcode ensuring the device is always locked
- Disable the message notifications on the device lock-screen
- Enable the remote wipe feature should the device be lost or stolen
- Never allow their device to be shared
- Enable two-step verification
- Review any links to other instant messaging apps and determine whether they need to be turned off

When using an IM for organisation related matters, staff must ensure they are considerate of their co-workers and are not to:

- Use foul or abusive language

- Send discriminatory and/or derogatory information including information based on sex, age, race, religion, politics, etc., regardless of whether the information was intended as a 'joke'

- Share links or refer to pornography, gambling, the promotion of terrorism or terrorism skills or cult-promoting paraphernalia

Staff are reminded that, should they lose their device, this could have both personal and professional ramifications and therefore they must ensure they adhere to the requirements outlined above.

Should staff be communicated with outside of their normal working hours, ordinarily there is no expectation that this is to be responded to during non-working times. For some business-critical positions this might be a requirement.

7 Intranet and clinical system

7.1 Usage

Staff must ensure that, when accessing information on the intranet, confidentiality is always maintained, ensuring that access by unauthorised persons is prevented.

Any unauthorised access constitutes a security breach and must be reported to the Information Governance Lead immediately.

7.2 Access

Staff are not permitted to use the intranet and/or the clinical system to access any medical information relating to themselves, their families, colleagues or friends unless this has been authorised by the appropriate manager and deemed legitimate.

Unauthorised access is absolutely forbidden and will be considered to be a disciplinary offence, and the appropriate disciplinary action will be taken against offenders.

7.3 Appropriate content

As for instant messaging, staff must not access and/or send discriminatory and/or derogatory information using the organisation's intranet or email systems.

The sending of discriminatory or derogatory information is a disciplinary offence and appropriate disciplinary action will be taken against offenders.

8 Tele and videoconference consultations

8.1 Tele and videoconferencing governance

Another form of communication can be achieved via a tele or videoconference consultation call. NHS England has established information regarding the use of this technology when supporting patient access in its detailed document titled Using video conferencing and consultation tools.

Managing the risks associated with tele and videoconferencing needs attention from both care professionals and service users and guidance to support risk assessments can be found in the Health, Safety and Risk Management Handbook.

Further information can be sought from the Audio Visual and Photography Policy.

8.2 Patient considerations

When assessing suitability for tele and videoconferencing, the following is to be considered:

- The healthcare professional will ensure that the decision as to whether tele and/or videoconferencing is a suitable form of communication will always be considered on an individual patient basis

- The healthcare professional will always assess the appropriateness of any tele and/or videoconference consultation and it will be their professional judgement regardless of any patient request

- Should there be any concern regarding risk, neglect or any other safeguarding issue, then consideration must be given to the appropriateness of tele and/or videoconferencing due to the lack of guarantee as to whether the patient is alone and is able to give a full account of the reasons for the consultation. In this instance, the patient would be offered a face to face appointment and the clinician should refer to The Safeguarding Handbook

- Tele and/or videoconferencing will not be considered for those patients when the matters to be discussed may cause the patient distress or anxiety or to discuss matters of sensitivity, such as informing an individual that they have been diagnosed with a terminal illness or potentially stigmatising condition

- Patients are to be made aware that no communication over the internet is entirely secure

- While tele and/or videoconferencing can bring benefits to both patients and this organisation, such as convenience, less travel and cost savings, it should be offered as a choice rather than a requirement. It should not be offered when care may be undermined or when service users may struggle to cope

- Patients are to be made aware that they will need to have a good quality internet connection to achieve the most benefit out of the videoconferencing service

- The patient is to be advised that the organisation cannot provide any guarantees as to the quality or security of the service; neither can any support be provided to resolve technical issues

8.3 Patient consent to videoconferencing

Patient consent to the use of videoconferencing is required but need not be explicit. Annex D details the videoconference consent form.

9 Artificial intelligence systems

9.1 About

The use of innovative technologies such as Artificial intelligence Systems (AIS) within healthcare is becoming more prevalent. Within general practice, the likelihood is that the main use would be as a tool to support in the writing of patient consultations, or in a letter to a patient, for example following a complaint.

While the use of Artificial Intelligence (AI) aims to enhance the accuracy of documentation, reduce administrative workload and increase and improve patient engagement, consideration has to be given to the protection of patient data, upholding professional standards and ensuring compliance with legal and ethical responsibilities.

Considerations of both the pros and cons of AI are detailed at Section 9.4.

The NHS document titles All adopters guidance lists all the requirements and regulations that apply to adopters of digital technologies within any health and social care setting. Further detailed reading can be found in the NHS E guidance titled Artificial Intelligence: How to get it right.

9.2 Information governance and compliance

When considering the information governance (IG) implications, there is a need to be clear about ensuring the criteria within the Data Protection Act 2018 is being met.

In particular:

- What data is required?
- Why is it required?
- Who will be processing it and will it be shared?
- How will it processed?
- Where will it be processed?

A Data Protection Impact Assessment (DPIA) will be required to be undertaken as this would capture potential impacts, consider mitigations and enable informed risk management. A DPIA template can be found in the UK GDPR Policy.

Following a DPIA, consideration is then to be given towards having a governance plan which is detailed within the MDU guidance titled Adopting AI in healthcare. In particular, if adopting a system that is already developed, the British Standards guidelines within this MDU link are to be complied with to ensure the stringent NHS data protection standards continue to be met.

It is imperative that no patient identifiable information is provided to support any AI data search and that the NHS Confidentiality Code of Practice is being complied with.

Retention of any AI data is as for other healthcare records and as detailed within the Record Retention Schedule document.

To ensure that risks have been considered and mitigated, prior to establishing AIS at this organisation, a risk assessment will be conducted. Further guidance can be sought within the Health, Safety and Risk Management Handbook.

9.3 Staff training and guidance

The use of and signing up to any AI tools can only be used after having obtained the explicit, written consent of the Partners or management. Unauthorised use of AI services will be considered a serious breach that may result in disciplinary action. The Practice Manager will maintain a list of those who are permitted to use AI technology.

There is a continued requirement for all staff to undertake mandatory training to support data protection. Furthermore, all staff are to be aware of the various supporting policies, including the procedures for reporting confidentiality breaches or suspected misuse.

Useful guidance including staff obligations and links to the various data protection policies can be found in the following:

- Data Security and Protection Toolkit Handbook
- Confidentiality and Data Protection Handbook

9.4 Benefits and pitfalls of using AI technology

While not an exhaustive list, the following table details some of the pros and cons of using AI within a consultation:

Pros	Improved documentation accuracy	Reduces human error in note-taking, providing detailed and accurate records of consultations
	Better time management	Cuts down administrative tasks, enabling clinicians to see more patients or focus on quality care
	Enhanced patient interaction	Allows clinicians to concentrate on patients with AI managing the documentation
	Standardisation of notes	Ensures consistency in record-keeping and may potentially enable quicker access to notes for clinical or audit purposes
Cons	Implementing governance	There is a requirement to ensure that any AI systems are implemented and used safely. These must comply with DPA18, British Standards and NHS data protection requirements. Data storage and processing locations are to be confirmed. These can sometimes be hidden in lengthy terms and conditions or data processing agreements. Of note, in some cases, the data submitted by practices could be used beyond the original intention, including to train AI models.
	Potential data privacy risks	The use of AI in handling patient data introduces risks if data transmission or storage is not secure.
	Information ownership	Any data entered into AI then becomes the property of the AI company. It is then likely that this information will become available for other AI users. For the appropriate result, any search may require data inputting detailed, specific and even sensitive patient information that could compromise a patient's data security.
	Reliance on technology	Dependence on AI could reduce note-taking skills which may be an issue if the system is unavailable.
	Time factor	There is a time element to train and standardise any use of AI technology throughout the team. Furthermore, time will be needed to undertake regular audits ensuring controls and measures are being maintained.

	Risk of misinterpretation	AI may misinterpret patient information, especially in complex or nuanced cases, leading to potential inaccuracies. AI can often appear vague and impersonal.
	Confirmation of correctness and wording	All AI produced documents would still require human interaction to check for empathy and content. Many AI companies use US spellings, phrases and terminology. Content may be generalised and as such would need to comply with current healthcare governance requirements specific to the UK.
	Financial costs	The initial setup and ongoing costs of AI may impact the practice's budget.

Additional reading can be found at:

- MDU guidance titled Can I use AI to write a complaint response?
- Practice Index blog titled AI in general practice – striking the right balance

9.5 Monitoring and review

Should there be any changes in data protection regulations or advances in AI technology, this guidance will be reviewed.

When AI is used, then this will form part of any data protection audits, including the annual Data Security and Protection Toolkit (DSPT) return to confirm that the security of any technology that is being used is both appropriate and being maintained. Any shortcomings following an audit, or any incidents involving AI will be documented and reviewed to identify risks and implement improvements.

10 Telephone communications

10.1 Provision

Telephones are provided to enable staff to communicate with patients, patients' carers and other service providers to ensure that the expected level of service is always delivered.

Further reading can be found in the Correspondence Management Policy.

10.2 Acceptable and authorised use

The practice telephones are only to be used for the purpose of the organisation's business. Personal use is strictly prohibited except in the event of an emergency. Calls to premium-rate telephone numbers are also prohibited.

Calls to areas outside the UK are blocked; should it be necessary to call a number, Practice Manager authorisation will be required.

10.3 Recording incoming and outgoing calls

In accordance with the UK GDPR, the lawful basis for processing data also applies to the recording of telephone calls. To conform with this in relation to the recording of telephone calls, one of the processing requirements as detailed within Article 6 must apply.

When accepting an incoming call or dialling out, staff must advise the caller or receiver that the call will be recorded and give the reason for the call being recorded. Should any call then be listened to, say for training purposes, then this detail is to be entered into a Telephone Call Recording Register.

Information that is required is:

- Who has accessed the call
- Reasons why
- What was done with the recording

A template Recordings Register can be found at Annex E.

Further guidance can be sought from the Audio Visual and Photography Policy.

At this organisation, the data controller is responsible for and must be able to demonstrate compliance with the principles relating to the processing of personal data as outlined in Article 5 of the UK GDPR.

10.4 General guidance to answering the telephone

The following sequence is standard when answering the telephone to verify the details of the caller:

- Use the appropriate salutation
- State your name and the name of the organisation
- Ask who is calling and the nature of the call
- Activate the silence button when appropriate
- Always be polite and professional

If not already within the preamble message, mention to the caller that calls are recorded with a justification such as training purposes.

10.5 Verifying a patient caller

Prior to any information being passed to a caller, the patient's identity is to be verified. Follow the options below to do this noting that only necessary information should be provided.

- Request that the patient confirms their name, address, date of birth and either home or mobile telephone number

- If unable to remember their telephone details, suggest that you will call back on one of their listed numbers or an alternative number that is listed for a proxy or next of kin

- If neither of the above can be satisfied, then the caller should be advised that no information can be passed due to their inability to verify who they are

Guidance on verifying online patient identification can be accessed at NHS E document titled Good Practice Guidance on Identity Verification.

10.6 Communicating with a relative

Information should not be divulged to anyone other than the patient unless consent has been given and is recorded in the patient's healthcare record on the clinical system.

Therefore, before any personal and/or sensitive information may be shared by telephone, it is the staff member's responsibility to ensure that the caller has the legal right to that information and that the subject of the information has provided consent.

This may include confirming the whereabouts of the patient.
Staff must therefore:

- When practicable, confirm the consent of the patient has been given and confirm that this has been recorded within the clinical notes
- Check the identity of caller and the patient's full name. This may involve telephoning the caller back to verify any listed telephone number

- Make sure the person they are talking to is entitled to the information

- If in any doubt, not provide any information until they are sure the information should be provided

- If unsure, pass the call to a senior member of staff

10.7 Communicating with a third party

Information may be provided to a third party should this be in the interest of patient care. To do this, the caller's identity must be verified following the below procedure:

- Request the patient's details to include three forms of identity. This could include their name, address, date of birth and either home or mobile telephone number

- Confirm the caller's telephone number, including any switchboard extension

- To verify the caller's identity, the number provided for the switchboard (hospital, police, social worker) should be called. Should the caller be phoning from a mobile, then ask the switchboard if this is the correct contact detail for this person prior to returning the call

- If unsure, the call should be passed to a senior member of staff

Reminder, this information can only be passed in the interest of patient care. Information should not be passed to other parties such as employers asking the whereabouts of their staff members.

10.8 Telephone messages for staff

If a call is received at the organisation for a member of staff and they are absent or busy, the person receiving the call is to record the following information:

- Name of caller
- Time of call
- Date of call
- Who they were calling/wanted to speak to
- Message (if applicable)
- The caller's telephone number (repeat this back to the caller for confirmation)
- An appropriate time to call back

This information is to be relayed to the intended recipient as soon as practicable.

NOTE: If a patient calls to discuss a care-related issue, this must be annotated in the patient's electronic healthcare record and the intended recipient informed.

10.9 Telephone messages for patients

To ensure that patient care is of the highest standard, information that is to be relayed to patients must be clear and comprehensible. At this organisation, the following process is to be followed:

- Clinicians are to send messages to staff using the clinical system to request that they contact the patient and relay the message while ensuring that the administrative staff have all the necessary information to give to the patient

- The clinician is to make an appropriate entry in the patient record that this has been done

- Once the member of administrative staff has relayed the message to the patient, they are to make an entry in the patient's record stating that the message has been passed to the patient with a short summary of the information that was relayed

- Any comment made by the patient is also to be recorded

10.10 Abusive or aggressive patients

Unfortunately, on occasion, there may be times when a patient calls the practice and speaks to a member of staff in an abusive or aggressive manner.

Staff must ensure that they:

- Annotate the date and time of the call
- Ascertain who is calling

- Remain calm, offering empathy
- Determine the reason (if possible) for the aggression or abuse
- Offer solutions if practicable
- Advise the caller that if they persist with such an aggressive and/or abusive tone, the call with be ended
- End the call if appropriate
- Note down a summary in the patient's healthcare record
- Inform the Practice Manager
- Report the incident in accordance with the practice incident reporting policy or significant event policy

In all circumstances, staff are to demonstrate confidence and compassion, remaining calm throughout the incident. Staff should refrain from being judgemental, instead opting to show the patient their clear intention to resolve the situation as opposed to attempting any form of reprimand.

Refer to the Dealing With Unreasonable Violent and Abusive Patients Policy and the Removal of Patients Policy.

10.11 Contacting the police

Should it be necessary to contact the local police, the organisation is required to notify the CQC as this is a statutory notification.

Statutory Notification - Police involvement incident notification form

11 Internal monitoring of communications and records

11.1 Monitoring electronic communications at work

For quality control and auditing purposes, all staff are reminded that a random percentage of all forms of communication will be monitored within this organisation. These audits will include correspondence between both staff to patient and staff to staff.

This measure is to support best practice and ultimately to improve upon the patient experience and any such monitoring will be logged within the Recordings Register at Annex E.

Detailed information to support this requirement, including a form that can be used to confirm understanding during the induction process can be found in the Staff Monitoring Policy.

11.2 Legitimate access of patient or staff records

Staff can access the clinical or personal employment records of patients or staff members for business purposes only. For staff employment records, strict access measures will be adopted and maintained. For clinical records, it is a breach of both the data protection legislation and common law duties of confidentiality to access any records for personal reasons.

Audits of the clinical system will be undertaken to ensure that there has been no inappropriate access to healthcare records.

Further supporting reading can be found in the following guidance documents:

- Staff Monitoring Policy
- Information Governance Breach Reporting Policy
- Confidentiality and Data Protection Handbook

12 Information from meetings

12.1 Accessibility and actions

Following internal meetings, the minutes will be written and saved within the relevant shared drive with the aim of all staff receiving an email with a hyperlink to the minutes within 48 hours of the meeting occurring.

Staff are to ensure that they access this information and read the relevant minutes in a timely manner, either the day of receiving the email or the following day or the day when they return to work following the meeting.

For reference or should staff members wish to be reminded of the outcome of a meeting, for ease, a copy of the minutes of the meeting will be available.

For meeting types and structures refer to the Practice Manager's Handbook.

13 Maintaining security and general requirements

13.1 Standard security IT procedures

The following procedures apply to all organisation IT hardware:

- All staff are to lock their device when leaving it unattended, no matter how brief their absence may be
- Staff must log out at the end of the working day and shut down the device
- Staff should ensure that login and password information is stored securely and not shared with anyone
- Staff should not attach external hard drives (including USBs) to any organisation device
- Any organisation portable device, e.g., laptop, tablet, mobile phone, etc., must be used and stored in accordance with the Portable Device Policy

13.2 Good practice

To preserve the life of the organisation's IT equipment, staff should adhere to the following guidance:

- Refrain from eating or drinking in the vicinity of devices
- Do not use excessive force or subject devices to severe or sudden impacts
- Ensure that portable devices are transported in the appropriate protective cases and as detailed within the Portable Device Policy
- Ensure systems are shut down at the end of the working day or when not in use for prolonged periods of time, i.e., long-weekend closure, etc.
- Conduct Display Screen Equipment assessments as detailed within the Eyesight and Display Screen Equipment Policy
- Provide access to IT as necessary
- Only use the locally approved IT department to resolve any IT related issues

13.3 Virus safeguarding

All staff must ensure that any files that are downloaded are virus checked before being used. Staff are not permitted to download/load software unless it is an officially approved software product.

Annex A – Preferences for email and text messaging service

PREFERENCES FOR RECEIVING EMAILS AND TEXT MESSAGES	
Patient full name:	
Date of birth:	
Patient address:	
Email address:	
Mobile telephone number:	

My email/text communication preferences are: (please tick all that apply):

Give consent for communication by email	
Give consent for communication by SMS text messaging	
Give consent to only receive the following via email or SMS:	
• Appointment reminders	
• Appointment letters	
• Individual invites to screening, medication reviews, vaccination appointments	
• Test result notifications/advice to call the practice when action is needed	
• Friends and family test surveys	
• Interactive messages with the ability to confirm/cancel appointments	
Declined consent to receive email or SMS text messaging	

I understand and agree with each statement (please tick):

I will be responsible for the security of the information that I receive	
If I choose to share my information with anyone else, this is at my own risk	
I will contact the practice as soon as possible if I suspect that my information has been accessed by someone without my agreement	
If I think that I may come under pressure to give access to someone else unwillingly I will contact the practice as soon as possible	

Signature:		**Date:**	

Annex B – Consent to proxy access for email or SMS

Note: If the patient does not have capacity to consent to grant proxy access and proxy access is considered by the practice to be in the patient's best interest, Section 1 of this form may be omitted

Section 1 – Patient declaration

- I…… (name of patient), give permission to Woodbrook Medical Centre to give the person/people indicated below proxy access to the text messaging services as indicated below in Section 2.

- I understand that I may reserve the right to reverse any decision I make in granting proxy access at any time

- I understand the risks of allowing someone else to have access this information

Signature of patient:		Date:	

Section 2 – Consent options

Give consent for communication by email	
Give consent for communication by SMS text messaging	
Give consent to only receive the following via email or SMS:	
• Appointment reminders	
• Appointment letters	
• Individual invites to screening, medication reviews, vaccination appointments	
• Test result notifications/advice to call the practice when action is needed	
• Friends and family test surveys	
• Interactive messages with the ability to confirm/cancel appointments	

Section 3 – The representatives

(These are the people seeking proxy access to the patient's online records, appointments or repeat prescription)

Surname		Surname	
First name		First name	
Date of birth		Date of birth	
Address		Address	

Postcode		Postcode	
Email		Email	
Telephone		Telephone	
Mobile		Mobile	

Section 4 –The patient (If the patient does not have capacity)

Surname		Date of birth	
First name			
Address			
		Postcode:	
Email address			
Telephone number		Mobile number	

Section 5 – Representative Declaration

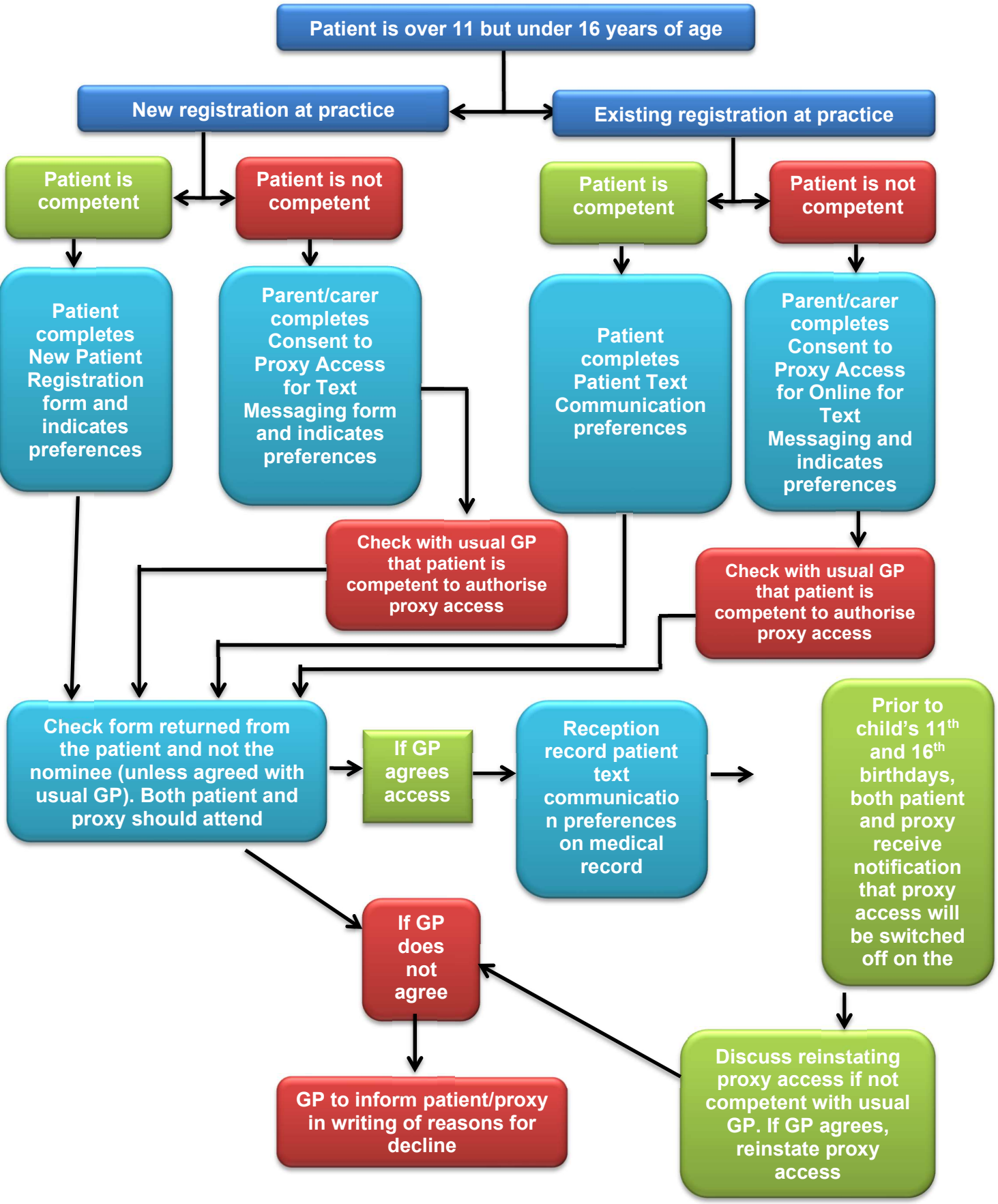
I/We ..... (names of representatives) wish to have access to the information ticked in the box above in Section 2 for ..... (name of patient)

I/We understand my/our responsibility for safeguarding sensitive information and understand and agree with each of the following statements:

I/We will be responsible for the security of the information that I/we see	
I/We will contact the practice as soon as possible if I/we suspect that the information has been accessed by someone without my/our agreement	

Signature(s) of representative(s):		Date(s):	
Signature(s) of representative(s):		Date(s):	

Annex C – Text messaging access process for 11 to 16 years



Annex D – Videoconferencing consent form

CONSULTATIONS BY VIDEOCONFERENCING	
Patient name:	
Date of birth:	
Patient address:	

Patients may be contacted via a remote video consultation service to save both time and expense. As such, [insert organisation name] can offer the trusted NHS [insert communication service] and if in agreement, it will contact you to discuss routine matters of care.

You do not have to use these services and you can still be seen in person by booking an appointment in the usual way. If you are interested in using this service, there are certain factors you should be aware of, including some risks.

Potential risks

- Online services send data across the internet in an encrypted format. This is a reasonably secure means of sending data, but it is not 100% secure.
- Poor quality internet connections can often interfere with the quality of the videoconference.

Required practice

- We will always call you for a tele or videoconference or send you instructions on how to join the call. You will not be asked, and should not attempt, to call the practice directly.
- Please use the fastest connection you have available (mobile or broadband) and the device with the highest resolution/quality webcam/rear facing camera.
- Should you wish to talk about matters that are particularly personal, confidential or sensitive, your healthcare professional may wish to establish a face-to-face follow up appointment. It is important that you understand this is in your best interests.
- Make sure that you have a safe, quiet, confidential place that is free from interruptions for your consultation.
- You should set your privacy preferences for receiving communications.
- If you wish to record the session with your own application or another device, we request that you inform our staff in advance.

I confirm that I have been made aware of the potential risks and I am happy for those directly involved with the provision of my care to contact me using videoconference.	
Patient telephone number	
Patient signature:	
Date (DD/MM/YY):	
Received by (name):	
Position:	
Signature:	
Date (DD/MM/YY):	

Annex E – Recordings Register

Date of request	Purpose	Reviewing person	Date/time of the recording	Person authorising release of information	Comments