|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | Created | | **Review Status** |
| 1.0 | February 2018 | Review Due February 2021 | |

**GDPR POLICY** – Consent

The General Data Protection Regulation (GDPR) will apply in the UK from May 2018 and replaces the Data Protection Act 1998 (DPA).

The GDPR sets a high standard for consent. It builds on the DPA standard of consent in a number of areas and it contains significantly more detail that codifies existing European guidance and good practice.

This policy details our approach to compliance and discusses what counts as valid consent. It also provides practical help to decide when to rely on consent, and when to look at alternatives. This policy relates to consent with regards to processing data only. For consent for providing medical treatment, please refer to the policy *Consent Policy - Medical Consent Including Treatment of Children*

# **About this policy**

This policy should be read in conjunction with the other GDPR related policies concerning data processing to give more detailed, practical guidance on consent under the GDPR.

The GDPR sets a high standard for consent. Consent means offering patients genuine choice and control over how we use their data. When consent is used properly, it helps us build trust and enhances our reputation.

This policy will explain when to rely on consent for processing and when to look at alternatives. It explains what counts as valid consent, and how to obtain and manage consent in a way that complies with the GDPR.

The policy sets out how the Information Commissioner’s Office (ICO) interprets the GDPR, and our general recommended approach to compliance and good practice.

# 

### Summary

* Consent must be unambiguous and involve a clear affirmative action.
* Consent should be separate from other terms and conditions. It should not generally be a precondition of signing up to a service.
* The practice will not use pre-ticked opt-in boxes.
* Granular consent is required for distinct processing operations.
* We must keep clear records to demonstrate consent.
* Patients have the right to withdraw consent, and we must offer them easy ways to withdraw consent at any time.
* If we have relied on consent for processing, patients have the right to erasure
* Consent should only be used as the legal basis for data processing, if there is no other alternative

### 

# **Why is consent important?**

### What role does consent play in the GDPR?

For processing to be [lawful](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/key-areas-to-consider/) under the GDPR, we need to identify (and document) our lawful basis for the processing. There are six lawful bases listed in Article 6(1), and consent is one of them. The others are:

* Contractual Necessity
* Compliance with Legal Obligations
* Vital Interests
* Public Interest or in exercise of official authority
* Legitimate interests. (This does not apply to public authority, and should therefore not be used by the practice as a legal basis for data-processing)

As an NHS organisation, it is likely that the majority of data processed by the practice will be health related. This is considered a special category (sensitive)

If you want to process special category (sensitive) personal data, you also need to apply one of the conditions in Article 9(2). ‘Explicit consent’ is one option for legitimising the use of special category data. The others are:

* Vital Interests
* Charity or not-for profit bodies
* Manifestly made public by data subject
* Legal Claims
* Substantial public interest
* Health and Social Care
* Public Health
* Historical, statistical or scientific purposes

Consent can also legitimise [restricted processing](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-restrict-processing/), and explicit consent can legitimise [automated decision-making](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/rights-related-to-automated-decision-making-and-profiling/) (including profiling), or [overseas](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/)  [transfers](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/) by private-sector organisations in the absence of adequate safeguards.

If you rely on consent, this will affect individuals’ rights. People will generally have stronger rights when processing is based on consent – for example, [the right to erasure](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/) (also known as ‘the right to be forgotten’) and the [right to data portability](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-data-portability/). It is therefore essential that consent is only used as the legal basis for data processing when there is no suitable alternative. In most instances where data is processed for the purpose of healthcare, consent is not required to be the legal basis.

Consent is only appropriate if we can offer patients real choice and control over how you use their data, and want to build their trust and engagement. But if you cannot offer a genuine choice, consent is not appropriate. If you would still process the personal data without consent, asking for consent is misleading and inherently unfair.

### What are the penalties for getting it wrong?

Making mistakes around consent could leave the practice at risk of substantial fines under the GDPR. Article 83(5)(a) states that infringements of the basic principles for processing personal data, including the conditions for consent, are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of total worldwide annual turnover, whichever is higher.

### When are we likely to require consent?

There will be times when it is appropriate to rely on consent as the legal basis. These include but are not exclusive to:

* Subject Access Requests
* Sharing information for research purposes
* Disclosing information to a third party
* Sharing information in an unexpected or intrusive way
* Sharing information for a purpose other than healthcare
* Sharing information for marketing purposes

In these instances consent should always be explicit. This means the patient (or their representative if they have legal authority, or parental responsibility), has signed a document to confirm they fully understand what information will be disclosed. There is more information on capacity & consent for children below.

### 

### Processing data without consent

If you would still process the data (e.g. record the details of a consultation) then consent cannot be the legal basis for processing the data. In this instance the patient cannot choose for information they have disclosed to the clinician to be omitted. It is also unlikely the information would be ever be erased, so the patient does not have a ‘choice’. In this instance, seeking consent from the patient is misleading and inherently unfair. Instead we should inform the patient of how we will process their data, to ensure fairness and transparency.

### Using Consent as the legal basis for data processing

The GDPR sets out requirements for using consent as a legal basis

* Consent must be freely given; this means giving patients genuine ongoing choice and control over how you use their data.
* Consent must specifically cover the controller’s name (the Practice). We must also name any third parties who will be relying on consent.
* Consent must cover the purposes of the processing and the types of processing activity. When required there should be granular options, e.g. we should list each separate part, and the patients should confirm consent for each
* Consent requests must be prominent, unbundled from other terms and conditions, concise and easy to understand, and user-friendly.
* Consent should be obvious and require a positive action to opt in.
* The patient has the right to withdraw consent at any time and we should provide details of how they can do this.
* Explicit consent must be expressly confirmed in words, rather than by any other positive action. Explicit consent should always be obtained when processing healthcare (sensitive) data.
* Information provided to patients should be prominent, concise and in plain language. It should not be included in ‘terms and conditions’ of service.
* There is no set time limit for consent. How long it lasts will depend on the context. You should review and refresh consent as appropriate.

### Unambiguous indication (by statement or clear affirmative action)

It must be obvious that the patient has consented, and what they have consented to. This requires more than just a confirmation that they have read terms and conditions – there must be a clear signal that they agree. If there is any room for doubt, it is not valid consent.

Therefore all consent documentation created by the practice should include tick boxes for the patient to “opt in” or have a clearly worded written statement for them to sign.

The practice will never use pre-ticked ‘opt in’ or ‘opt out’ boxes.

### 

### How long does consent last?

The GDPR does not set a specific time limit for consent. Consent is likely to degrade over time, but how long it lasts will depend on the context.

We need to consider the scope of the original consent and the individual’s expectation. If in doubt, please speak to the practice’s Data Protection Officer (DPO) or the Caldicott Guardian.

If the patient withdraws consent, we need to cease processing as soon as possible in the circumstances unless you have another lawful basis. This does not affect the lawfulness of the processing up to that point.

Parental consent will always expire when the child reaches the age at which they can consent for themselves. We therefore should review and refresh children’s consent at appropriate milestones. If in doubt, please speak to the practice’s Data Protection Officer (DPO) or the Caldicott Guardian.

### Capacity to consent?

The GDPR does not contain specific provisions on capacity to consent, but issues of capacity are bound up in the concept of ‘informed’ consent.

Generally, we can assume that adults have the capacity to consent unless we have reason to believe the contrary (e.g. diagnosis of dementia). If in doubt, you should speak to the Practice’s Caldicott Guardian.

It may be that you do have reason to believe that someone lacks the capacity to understand the consequences of consenting and so cannot give informed consent. If so, a third party with the legal right to make decisions on their behalf (eg under a Power of Attorney) can give consent. A copy of the POA should be stored in the medical record. We need to ensure that the POA relates to health and welfare, and not just property and financial affairs.

### Children’s consent

There are no global rules on children’s consent under the GDPR. If however, we are relying on consent rather than another lawful basis for the processing, we must get parental consent for all children under 13. For those 13 – 16 parental responsibility may still apply. You should therefore seek advice from the practice DPO or Caldicott Guardian if you have any doubt about the patient’s capacity to consent. They will consider whether the individual child has the competence to understand and consent for themselves (the ‘Gillick competence test’).

The practice needs to ensure there are age-verification measures in place for children, e.g. if we are registering a child who has not previously been registered with the NHS, you should ask to see the birth certificate or passport to confirm the age of the patient.

We are also expected to make ‘reasonable efforts’ to verify parental responsibility for those under the relevant age.

### 

### Writing a consent request

Consent requests need to be prominent, concise, easy to understand and separate from any other information such as general terms and conditions. All consents requests need to use clear, straightforward language, and adopt a simple style that patients find easy to understand – this is particularly important if you are asking children to consent. In this instance we need to prompt parental input and consider [age-verification and parental-](#_bookmark14)  [authorisation issues](#_bookmark14).

### What information should you include?

Consent must be [specific and informed](#_bookmark10). As a minimum a consent request must include:

* + - the name of the practice and the names of any third parties who will rely on the consent – consent for categories of third-party organisations will not be specific enough;
    - why you want the data (the purposes of the processing);
    - what you will do with the data (the processing activities); and
    - that the patient can withdraw their consent at any time. It is good practice to tell them how to withdraw consent.

### Just in time notices

You could also consider using ‘just-in-time’ notices. These work by appearing on-screen at the point the person inputs the relevant data, with a brief message about what the data will be used for. This will help you provide more information in a prominent, clear and specific way to ensure that consent is informed. However, you will need to combine the notices with an active opt-in and ensure this is not unduly disruptive to the user. This may be used booking appointments in the locality hub. The patient can give consent verbally in these situations, as long as they are fully informed. This consent should then be recorded in the patient record.

### What methods can you use to obtain consent?

Whatever method you use must meet the standard of an [unambiguous](#_bookmark11)  [indication by clear affirmative action](#_bookmark11). This means you must ask patients to actively opt in. Examples of active opt-in mechanisms include:

* + - signing a consent statement on a paper form;
    - ticking an opt-in box on paper or electronically;
    - clicking an opt-in button or link online;
* responding to an email requesting consent;
* answering yes to a clear oral consent request;
* volunteering optional information for a specific purpose – e.g. filling optional fields in a form

We cannot rely on silence, inactivity, pre-ticked boxes, opt-out boxes, default settings or a blanket acceptance of terms and conditions.

The GDPR does not specifically ban opt-out boxes but they are essentially the same as pre-ticked boxes, which are banned. Both methods bundle up consent with other matters by default, and then rely on inactivity. The usual reason for using opt-out boxes is to get more people to consent by taking advantage of inaction – but this is a clear warning sign of a problem with the quality of the consent. We should instead use specific opt-in boxes (or another active opt-in method) to obtain consent.

### 

### How should you record consent?

Article 7(1) says:

“*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*”

This means we must have an effective audit trail of how and when consent was given, so we can provide evidence if challenged. Our records must demonstrate the following:

* **Who consented:** the name of the individual, or other identifier (eg, online user name,

session ID).

* **When they consented:** a copy of a dated document, or online records that include an audit trail or timestamp; For oral consent there should always be a record of the time and date of the conversation.
* **What they were told at the time**: ideally a scanned copy of the document or a master copy of the data capture form containing the consent statement in use at that time, along with any separate privacy policy, including version numbers and dates matching the date consent was given. If consent was given orally, your records should include a copy of the script used at that time.
* **How they consented:** for written consent, a copy of the relevant document or data capture form. If consent was given online, the records should include the data submitted as well as a timestamp to link it to the relevant version of the data capture form. If consent was given orally, we should keep a note of this made at the time of the conversation - it doesn’t need to be a full record of the conversation.
* **Whether they have withdrawn consent:** and if so, when.

### 

### How should you manage consent?

We will require new consent if anything changes – for example, if the processing operations or purposes for requesting the information changes, the original consent may not be specific or informed enough.

If we relied on parental consent, we will also need to refresh consent as the children grow up and can consent for themselves. If we are in any doubt about whether the consent is still valid, speak to the DPO or Caldicott Guardian.

We should also consider whether to automatically refresh consent at appropriate intervals. How often it’s appropriate to do so will depend on the particular context, including patient’s expectations, whether they are in regular contact, and how disruptive repeated consent requests would be to the patient. In most cases we will refresh consent at a maximum of every two years

### How should you manage the right to withdraw consent?

The GDPR gives people a specific right to withdraw their consent, which can be done ‘at any time’. We should not make this in anyway difficult for patients. Withdrawal of consent can be made orally or in writing. We should ensure we record the withdrawal in the record, and this should include who has withdrawn consent, and the time and date of this. If possible, we should also record the reason why consent is being withdrawn.

The GDPR does not prevent a third party acting on behalf of an individual to withdraw their consent, but we need to be satisfied that the third party has the authority to do so.

If someone withdraws their consent, this does not affect the lawfulness of the processing up to that point. However, it does mean we can no longer rely on consent as the lawful basis for processing. We either need to stop the processing or identify [another lawful basis](#_bookmark6) and be able to justify why continued processing is fair.

We must include details of the right to withdraw consent in our privacy notices and consent requests.

**Related documents**

Related documents – available on the intranet

Flow chart – Simple guide to consent for data processing

Policy - Obtaining Online Access to Medical Records (including consent form) \*

Consent form – Access to medical records – NOT online access\*

Policy – Subject Access requests

Policy – Access for records - deceased patients (including consent form) \*

Word templates – available on EMIS

Consent request for private work

Consent for release of medical records to solicitor

\*also has section for proxy access

**Checklist**

## Asking for consent

* We have checked that consent is the most appropriate lawful basis for processing.
* We have made the request for consent prominent and separate from our terms and conditions.
* We ask people to positively opt in.
* We don’t use pre-ticked boxes, or any other type of consent by default.
* We use clear, plain language that is easy to understand.
* We specify why we want the data and what we’re going to do with it.
* We give granular options to consent to independent processing operations.
* We have named our practice and any third parties.
* We tell individuals they can withdraw their consent.
* We ensure that the individual can refuse to consent without detriment.
* We don’t make consent a precondition of a service.
* If we offer online services directly to children, we only seek consent if we have age-verification and parental-consent measures in place.

## Recording consent

* We keep a record of when and how we got consent from the individual.
* We keep a record of exactly what they were told at the time.

## Managing consent

* We regularly review consents to check that the relationship, the processing and the purposes have not changed.
* We have processes in place to refresh consent at appropriate intervals, including any parental consents.
* We make it easy for patients to withdraw their consent at any time, and publicise how to do so.
* We act on withdrawals of consent as soon as we can.
* We don’t penalise patients who wish to withdraw consent.