# Privacy Policy

Dr S Butler & Partners

| | |
|---|---|
| **Policy:** | **Privacy Policy** |
| **Date:** | **25th May 2020** |
| **Next Review Date:** | **25th May 2022** |
| **Policy Leads:** | **Dr S Butler & Partners – Data Controller**<br>**Mrs J Jackson – Data Protection Officer (for day to day Practice purposes)**<br>**Basildon and Brentwood Clinical Commissioning Group Data Protection Officer, Nohossan Kane, for advice & guidance** |

The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take 'appropriate measures'.

Data controllers may need to include more information in their privacy notices, but we believe that by following the good practice recommendations in this code we will be well placed to comply with the GDPR regime. There is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice and the Practice have chosen the format herein.

The GDPR says that the information we provide to people about how we process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

These requirements are about ensuring that privacy information is clear and understandable for data subjects. They also make explicit what has always been set out as good practice. Following the advice in this code about the use of language, about adopting innovative technical means for delivering privacy information such as layered and just in time notices, and about user testing will help us to comply with the new provisions of the GDPR, as well as the current requirements of the DPA. The explicit emphasis on adapting privacy notices for children goes beyond what is currently required by the DPA. Data controllers processing children's data will need to take account of the level of comprehension of the age groups involved and tailor their notices accordingly. The code seeks to address this in relation to making privacy notices accessible.

The GDPR includes a longer and more detailed list of information that must be provided in a privacy notice than the DPA does. There are also some differences in what we are required to provide, depending on whether we are collecting the information directly from data subjects or from a third party.

Following the advice in the code about planning, privacy notices and mapping our information flows gives us much of the detail we needed to meet these requirements.

***Appendix A to this policy gives specific measures to consider when sharing/consenting to share information regarding children***

# How Dr. S Butler & Partners (Western Road Surgery) uses your information to provide you with healthcare

## This practice keeps medical records confidential and complies with the General Data Protection Regulation.

**We hold your medical record so that we can provide you with safe care and treatment.**

**We will also use your information so that this practice can check and review the quality of the care we provide. This helps us to improve our services to you.**

- We will share relevant information from your medical record with other health or social care staff or organisations when they provide you with care. For example, we will share information when they refer you to a specialist in a hospital or local community service; we will send details about your prescription to your chosen pharmacy; we may share your details with our Clinical Commissioning Group when you require individual funding for certain treatment or procedures etc.
- Information on how we share your information with organisations who are directly involved in your care can be requested from the Practice if needed. As a general rule, we usually try to share your medical information by e-referral to the relevant body or by sharing your GP record through the clinical system we use known as SystmOne (TPP). Both methods for sharing your information are secure and all NHS personnel are subject to codes of ensuring confidentiality and maintaining a high level of information governance.
- Healthcare staff working in A&E and out of hours care will also have access to your information. For example, it is important that staff who are treating you in an emergency know if you have any allergic reactions. This will involve the use of your Summary Care Record. You will have previously opted in to allow consent for us to undertake this. If you choose or now wish to withdraw consent please speak to one of the Receptionists and request a Summary Care Record Opt Out Form. For more information see: https://digital.nhs.uk/summary-care-records
- You may also choose to opt out of allowing NHS Digital to extract and provide your information to other parties for research etc. For more information or to opt out, please go to https://www.nhs.uk/your-nhs-data-matters
- You have the right to object to information being shared for your own care. Please speak to the Practice Manager if you wish to object. You also have the right to request to have any mistakes or errors corrected.

## Other important information about how your information is used to provide you with healthcare

### Registering for NHS care

- All patients who receive NHS care are registered on a national database.

- This database holds your name, address, date of birth and NHS Number but it does not hold information about the care you receive.

- The database is held by NHS Digital a national organisation which has legal responsibilities to collect NHS data.

- More information can be found at: https://digital.nhs.uk/ or the phone number for general enquires at NHS Digital is 0300 303 5678

## Identifying patients who might be at risk of certain diseases

- Your medical records will be searched by a computer programme so that we can identify patients who might be at high risk from certain diseases such as heart disease or unplanned admissions to hospital.

- This means we can offer patients additional care or support as early as possible.

- This process will involve linking information from your GP record with information from other health or social care services you have used.

- Information which identifies you will only be seen by this practice although there are some circumstances where this information will be shared. Please see the section regarding National Screening Programmes or view the website https://www.gov.uk/topic/population-screening-programmes

## Safeguarding

- Sometimes we need to share information so that other people, including healthcare staff, children or others with safeguarding needs, are protected from risk of harm.

- These circumstances are rare.

- We do not need your consent or agreement to do this.

- Please see the Essex Safeguarding Children Board website by which we follow and are guided for our policy making http://www.escb.co.uk

- There may also be times when we need to share information with relevant agencies with regards to vulnerable adults. This is for their own safety and where we feel they may be at risk. Where there is capacity consent will be sought from you to undertake this.

# How your information is used for medical research and to measure the quality of care

We sometimes share information from medical records:

- to support medical research when the law allows us to do so, for example to learn more about why people get ill and what treatments might work best;
- to participate in National Audit Programmes
- we will also use your medical records to carry out research within the practice.

This is important because:

- the use of information from GP medical records is very useful in developing new treatments and medicines;
- medical researchers use information from medical records to help answer important questions about illnesses and disease so that improvements can be made to the care and treatment patients receive.

We only share information for medical research with your explicit consent unless there is a national programme for sharing information with regards to a specific condition such as Diabetes. Where the programme is national then we are allowed to share data by automatic and electronic extraction from our clinical software programme. This data is sent to NHS Digital a National body with legal responsibilities to collect such data.

You have the right to object to your identifiable information being used or shared for medical research purposes. Please speak to the practice if you wish to object

## How your information is shared so that this practice can meet legal requirements

The law requires us to share information from your medical records in certain circumstances. Information is shared so that the NHS or Public Health England can, for example:

- plan and manage services;
- check that the care being provided is safe;
- prevent infectious diseases from spreading.

We will share information with NHS Digital, the Care Quality Commission, Basildon & Brentwood Clinical Commissioning Group, NHS England and local health protection team (or Public Health England) when the law requires us to do so. Please see below for more information.

We must also share your information if a court of law orders us to do so.

## NHS Digital

- NHS Digital is a national body which has legal responsibilities to collect information about health and social care services.

- It collects information from across the NHS in England and provides reports on how the NHS is performing. These reports help to plan and improve services to patients.

- This practice must comply with the law and will send data to NHS Digital, for example, when it is told to do so by the Secretary of State for Health or NHS England under the Health and Social Care Act 2012.

- More information about NHS Digital and how it uses information can be found at: https://digital.nhs.uk/home

## Care Quality Commission (CQC)

- The CQC regulates health and social care services to ensure that safe care is provided.

- The law says that we must report certain serious events to the CQC, for example, when patient safety has been put at risk.

- For more information about the CQC see: http://www.cqc.org.uk/

## Public Health

- The law requires us to share data for public health reasons, for example to prevent the spread of infectious diseases or other diseases which threaten the health of the population.

- We will report the relevant information to local health protection team or Public Health England.

For more information about Public Health England and disease reporting see:
https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report

## Basildon & Brentwood Clinical Commissioning Group & NHS England

- Your name, NHS number, Date of Birth, Address and medical details that relate to the need for an application to be made on your behalf for specialist funding known as an individual funding request

- Your NHS number or hospital number in cases where we need further information or query information received from a hospital or service provider that has been commissioned by the Clinical Commissioning Group i.e. Basildon Hospital

- Invoice validation is an important process. It involves using your NHS number for the CCG or NHS England, who are responsible for paying for your treatment. Section 251 of the NHS Act 2006 provides a statutory legal basis to process data for invoice validation purposes. We can also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

- CCGs support local GP practices with a Medicines Management Team who help with prescribing queries which generally don't require identifiable information unless they are having to approach or seek specific forms/brands of medication on our behalf for you. Where specialist support is required e.g. to order a drug that comes in solid form, in gas or liquid, the CCG medicines management team may order this on behalf of the practice to support your care.

## National screening programmes

- The NHS provides national screening programmes so that certain diseases can be detected at an early stage.

- These screening programmes include bowel cancer, breast cancer, cervical cancer, aortic aneurysms and a diabetic eye screening service.

- The law allows us to share your contact information with Public Health England so that you can be invited to the relevant screening programme.

- More information can be found at: https://www.gov.uk/topic/population-screening-programmes or speak to the practice.

## We are required by law to provide you with the following information about how we handle your information

| | |
|---|---|
| **Data Controller** contact details | Dr S Butler of Dr S Butler & Partners, Western Road Surgery, 41 Western Road, Billericay, Essex. CM12 9DX<br>Telephone: 01277 658117<br>Fax: 01277 658117<br>Email: admin.mailboxf81013@nhs.net |
| **Data Protection Officers** contact details | Mrs J Jackson, Practice Manager, Dr S Butler & Partners, Western Road Surgery, 41 Western Road, Billericay, Essex. CM12 9DX<br>Telephone: 01277 624599<br>Email: iulie.jackson4@nhs.net<br><br>Nohassan Kane, Data Protection Officer, Basildon and Brentwood Clinical Commissioning Group, Phoenix Court, Christopher Martin Road, Basildon, Essex, SS14 3HG<br>Tel: 01268 594 393<br>Email: nohossan.kane1@nhs.net |
| **Purpose** of the processing | • To give direct health or social care to individual patients.<br><br>• For example, when a patient agrees to a referral for direct care, such as to a hospital or community service, relevant information about the patient will be shared with the other healthcare staff to enable them to give appropriate advice, investigations, treatments and/or care.<br><br>• To check and review the quality of care. (This is called audit and clinical governance). |

**Lawful basis** for processing

These purposes are supported under the following sections of the GDPR:

*Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'; and*

*Article 9(2)(h) 'necessary for the purposes of preventative or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services..."*

**Recipient or categories of recipients** of the processed data

Healthcare staff will also respect and comply with their obligations under the common law duty of confidence.

The data will be shared with:

- Healthcare professionals and staff in this surgery and those attached to the surgery who operate from these premises such as the community midwife
- Local community services
- out of hours services;
- diagnostic and treatment centres;
- or other organisations involved in the provision of direct care to individual patients.

**Organisations Locally** - Listed below are some of the organisations we will share data with as detailed above however this list is not exhaustive:

Basildon & Thurrock University Foundation Hospital Trust
Brentwood Community Hospital
Queens Hospital
Essex Partnership University Hospital Trust (EPUT)
North East London Foundation Hospital Trust (NELFT)
St Lukes Hospice (One Response Team/End of Life Team)
Essex Social Services

**Rights to object**

- You have the right to object to information being shared between those who are providing you with direct care.

- This may affect the care you receive – please speak to the practice.
- You are not able to object to your name, address and other demographic information being sent to NHS Digital.
- This is necessary if you wish to be registered to receive NHS care.
- You are not able to object when information is legitimately shared for safeguarding reasons.
- In appropriate circumstances it is a legal and professional requirement to share information for safeguarding reasons. This is to protect people from harm.
- The information will be shared with the local safeguarding service under Essex County Council.

**Right to access and correct**

- You have the right to access your medical record and have any errors or mistakes corrected. Please ask to speak to one of the Secretaries in the first instance or look at our 'subject access request

SUBJECT ACCESS REQUESTS.pdf

- We are not aware of any circumstances in which you will have the right to delete correct information from your medical record; although you are free to obtain your own legal advice if you believe there is no lawful purpose for which we hold the information and contact us if you hold a different view.

**Retention period**

GP medical records will be kept in line with the law and national guidance. Information on how long records are kept can be found at: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016
or speak to the practice.

**Right to complain**

You have the right to complain to the Information Commissioner's Office. If you wish to complain follow this link https://ico.org.uk/global/contact-us/ or call the helpline **0303 123 1113**

**Data we get from**

We receive information about your health from other organisations

| | |
|---|---|
| **other organisations** | who are involved in providing you with health and social care. For example, if you go to hospital for treatment or an operation the hospital will send us a letter to let us know what happens. This means your GP medical record is kept up-to date when you receive care from other parts of the health service. |

**Appendix 1**

## Considering children when sharing/consenting to data processing/release - At a glance

- Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.
- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing, when offering an online service directly to a child, in the UK only children aged 13 or over are able to provide their own consent.
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.
- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- You should not usually make decisions based solely on automated processing about children if this will have a legal or similarly significant effect on them.
- You should write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

## Checklists

### General

☐ We comply with all the requirements of the GDPR, not just those specifically relating to children and included in this checklist.

☐ We design our processing with children in mind from the outset, and use a data protection by design and by default approach.

☐ We make sure that our processing is fair and complies with the data protection principles.

☐ As a matter of good practice, we use DPIAs to help us assess and mitigate the risks to children.

☐ If our processing is likely to result in a high risk to the rights and freedom of children then we always do a DPIA.

☐ As a matter of good practice, we take children's views into account when designing our processing.

**Bases for processing a child's personal data**

☐ When relying on consent, we make sure that the child understands what they are consenting to, and we do not exploit any imbalance of power in the relationship between us.

☐ When relying on 'necessary for the performance of a contract', we consider the child's competence to understand what they are agreeing to, and to enter into a contract.

☐ When relying upon 'legitimate interests', we take responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place.

**Offering an information Society Service (ISS) directly to a child, on the basis of consent**

**(Based on using SystmOne online service/NHS App)**

☐ If we decide not to offer our ISS (online service) directly to children, then we mitigate the risk of them gaining access, using measures that are proportionate to the risks inherent in the processing.

☐ When offering ISS to UK children on the basis of consent, we make reasonable efforts (taking into account the available technology and the risks inherent in the processing) to ensure that anyone who provides their own consent is at least 13 years old.

☐ When offering ISS to UK children on the basis of consent, we obtain parental consent to the processing for children who are under the age of 13, and make reasonable efforts (taking into account the available technology and risks inherent in the processing) to verify that the person providing consent holds parental responsibility for the child.

☐ When targeting wider European markets we comply with the age limits applicable in each Member State.

☐ We regularly review available age verification and parental responsibility verification mechanisms to ensure we are using appropriate current technology to reduce risk in the processing of children's personal data.

☐ We don't seek parental consent when offering online preventive or counselling services to a child.

**Marketing (In practice context marketing is for contacting children about child/young people services such as smoking cessation, sexual health campaigns, etc.)**

☐ When considering targeting marketing at children we take into account their reduced ability to recognise and critically assess the purposes behind the processing and the potential consequences of providing their personal data.

☐ We take into account sector specific guidance on marketing, such as that issued by the Advertising Standards Authority, to make sure that children's personal data is not used in a way that might lead to their exploitation.

☐ We stop processing a child's personal data for the purposes of direct marketing if they ask us to.

☐ We comply with the direct marketing requirements of the Privacy and Electronic Communications Regulations (PECR).

**Solely automated decision making (including profiling)**

☐ We don't usually use children's personal data to make solely automated decisions about them if these will have a legal, or similarly significant effect upon them.

☐ If we do use children's personal data to make such decisions then we make sure that one of the exceptions in Article 22(2) applies and that suitable, child appropriate, measures are in place to safeguard the child's rights, freedoms and legitimate interests.

☐ In the context of behavioural advertising, when deciding whether a solely automated decision has a similarly significant effect upon a child, we take into account: the choices and behaviours that we are seeking to influence; the way in which these might affect the child;

and the child's increased vulnerability to this form of advertising; using wider evidence on these matters to support our assessment.

☐ We stop any profiling of a child that is related to direct marketing if they ask us to.

**Data Sharing**

☐ We follow the approach in the ICO's Data Sharing Code of Practice and the IG Policies in place at the Practice.

**Privacy notices**

☐ Our privacy notices are clear, and presented in plain, age-appropriate language.

☐ We can use child friendly ways of presenting privacy information, such as: diagrams, cartoons, and graphics, icons and symbols where necessary.

☐ We explain to children why we require the personal data we have asked for, and what we will do with it, in a way which they can understand.

☐ As a matter of good practice, we explain the risks inherent in the processing, and how we intend to safeguard against them, in a child friendly way, so that children (and their parents) understand the implications of sharing their personal data.

☐ We tell children what rights they have over their personal data in language they can understand.

**The child's data protection rights**

☐ We design the processes by which a child can exercise their data protection rights with the child in mind, and make them easy for children to access and understand.

☐ We allow competent children to exercise their own data protection rights.

☐ If our original processing was based on consent provided when the individual was a child, then we comply with requests for erasure whenever we can.

☐ We design our processes so that, as far as possible, it is as easy for a child to get their personal data erased as it was for them to provide it in the first place.

**In brief**

**What's new?**

**A child's personal data merits particular protection under the GDPR.**

If you rely on consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over are able provide their own consent. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so. For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service. You must also make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

Children also merit specific protection when you are collecting their personal data and using it for marketing purposes or creating personality or user profiles.

You should not usually make decisions about children based solely on automated processing if this will have a legal or similarly significant effect on them. The circumstances in which the GDPR allows you to make such decisions are limited and only apply if you have suitable measures to protect the interests of the child in place.

You must write clear and age-appropriate privacy notices for children.

The right to have personal data erased is particularly relevant when the individual gave their consent to processing when they were a child.

What should our general approach to processing children's personal data be?

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

If you process children's personal data, or think that you might, then you should consider the need to protect them from the outset, and design your systems and processes with this in mind.

Fairness, and compliance with the data protection principles, should be central to all your processing of children's personal data.

It is good practice to consider children's views when designing your processing.

**What do we need to consider when choosing a basis for processing children's personal data?**

As with adults, you need to have a lawful basis for processing a child's personal data and you need to decide what that basis is before you start processing. You can use any of the lawful bases for processing set out in the GDPR when processing children's personal data. But for some bases there are additional things you need to think about when your data subject is a child.

If you wish to rely upon consent as your lawful basis for processing, then you need to ensure that the child can understand what they are consenting to, otherwise the consent is not 'informed' and therefore is invalid. There are also some additional rules for online consent.

If you wish to rely upon 'performance of a contract' as your lawful basis for processing, then you must consider the child's competence to agree to the contract and to understand the implications of the processing.

If you wish to rely upon legitimate interests as your lawful basis for processing you must balance your own (or a third party's) legitimate interests in processing the personal data against the interests and fundamental rights and freedoms of the child. This involves a judgement as to the nature and purpose of the processing and the potential risks it poses to children. It also requires you to take appropriate measures to safeguard against those risks.

**What are the rules about an ISS and consent?**

Consent is not the only basis for processing children's personal data in the context of an ISS.

If you rely upon consent as your lawful basis for processing personal data when offering an ISS directly to children, in the UK only children aged 13 or over can consent for themselves. You therefore need to make reasonable efforts to verify that anyone giving their own consent in this context is old enough to do so.

For children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling

service. You must make reasonable efforts (using available technology) to verify that the person giving consent does, in fact, hold parental responsibility for the child.

You should regularly review the steps you are taking to protect children's personal data and consider whether you are able to implement more effective verification mechanisms when obtaining consent for processing.

**What if we want to target children with marketing?**

Children merit specific protection when you are using their personal data for marketing purposes. You should not exploit any lack of understanding or vulnerability.

They have the same right as adults to object to you processing their personal data for direct marketing. So you must stop doing this if a child (or someone acting on their behalf) asks you to do so.

If you wish to send electronic marketing messages to children then you also need to comply with the Privacy and Electronic Communications Regulations 2003.

**What if we want to profile children or make automated decisions about them?**

In most circumstances you should not make decisions about children that are based solely on automated processing, (including profiling) if these have a legal effect on the child, or similarly significantly affect them. If you do make such decisions you need to make sure that you put suitable measures in place to protect the rights, freedoms and legitimate interests of the child.

If you profile children then you must provide them with clear information about what you are doing with their personal data. You should not exploit any lack of understanding or vulnerability.

You should generally avoid profiling children for marketing purposes. You must respect a child's absolute right to object to profiling that is related to direct marketing, and stop doing this if they ask you to.

It is possible for behavioural advertising to 'similarly significantly affect' a child. It depends on the nature of the choices and behaviour it seeks to influence.

**What about data-sharing and children's personal data?**

If you want to share children's personal data with third parties then you need to follow the advice in our data sharing Code of Practice. We also recommend that you do a DPIA.

**How do the exemptions apply to children's personal data?**

The exemptions apply to children's personal data in the same way as they apply to adults' personal data. They may allow you to process children's personal data in ways that the GDPR would not otherwise allow. You need to consider and apply the specific provisions of the individual exemption.

**How does the right to be informed apply to children?**

You must provide children with the same information about what you do with their personal data as you give adults. It is good practice to also explain the risks inherent in the processing and the safeguards you have put in place.

You should write in a concise, clear and plain style for any information you are directing to children. It should be age-appropriate and presented in a way that appeals to a young audience.

**What rights do children have?**

Children have the same rights as adults over their personal data which they can exercise as long as they are competent to do so. Where a child is not considered to be competent, an adult with parental responsibility may usually exercise the child's data protection rights on their behalf.

**How does the right to erasure apply to children?**

Children have the same right to have their personal data erased as adults. This right is particularly relevant when an individual originally gave their consent to processing when they were a child, without being fully aware of the risks.

One of the specified circumstances in which the right to erasure applies is when you collected the personal data of a child under the lawful basis of consent, when offering an ISS directly to a child.

It should generally be as easy for a child to exercise their right to erasure as it was for them to provide their personal data in the first place.