Direct Marketing Protocol

|  |  |  |
| --- | --- | --- |
| Policy Title / Reference | Author | Owner |
| Direct Marketing Protocol | Emma Cooper, Cluster DPO (Kafico) | Practice Manager |

|  |  |  |
| --- | --- | --- |
| Version | Revision author | Version comments |
| 1 | Emma Cooper, Kafico Ltd | Jan 18 New Draft |
| 1.1 | Emma Cooper, Kafico Ltd | Jan 19 Replaced 1998 DPA with 2018 Act. Replaced GDPR with “data protection legislation”.  Added section for patient texts and legitimate interests assessment in appendix. |

Contents

[2. Scope 2](#_Toc6746759)

[3. Definitions 3](#_Toc6746760)

[4. Introduction 3](#_Toc6746761)

[5. Statutory Mandatory Framework 3](#_Toc6746762)

[6. Accountable Parties 3](#_Toc6746763)

[7. Application of Protocol 4](#_Toc6746764)

[8. Lawful Basis for Direct Marketing 4](#_Toc6746765)

[9. Opt in / Out Out 4](#_Toc6746766)

[10. Texting Patients 5](#_Toc6746767)

[11. Associated Protocols 6](#_Toc6746768)

[12. Audit Schedule 6](#_Toc6746769)

[13. Review 6](#_Toc6746770)

[Appendix A 7](#_Toc6746771)

[Appendix B Texting Patients about Appointments and Services (GDPR Recital 47 Legitimate Interests Assessment) 9](#_Toc6746772)

# Scope

This protocol has been drafted for use by customers of Kafico Ltd across Suffolk.

At the time of writing and unless alternative protocols have been adopted locally, the protocol applies to;

|  |  |  |
| --- | --- | --- |
| Barrack Lane | Martlesham | Mendlesham |
| Burlington Road | Ravenswood | Wickhambrook |
| Framlingham | Stanton (west) | Church Farm Surgery (Aldeburgh) |
| Botesdale Health Centre | The Birches | Framfield |
| Felixstowe Road | Mount Farm | Saxmundham |
| Hawthorn Drive | Swan and Forest | Guildhall & Barrow |
| The Surgery, Leiston | Glemsford | Peninsula |
| Victoria Surgery | Lakenheath | Little St John Street |
| Ivry Street | Ixworth | Grove Medical Centre |

# Definitions

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

# Introduction

This protocol intends to support **Practice** staff in complying with the relevant legislation with respect to direct marketing to its customers and users.

# Statutory Mandatory Framework

This protocol supports the navigation of a complex framework of privacy legislation including Data Protection legislation, Common Law Duty of Confidence, Article 8 European Convention of Human Rights and the e-Privacy Directive.

# Accountable Parties

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure that information is processed in a fair and appropriate manner. Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

# Application of Protocol

The rules of direct marketing apply whether you are marketing to individuals or to businesses – as long as Personal Data is being used.

This means if you can identify an individual either directly or indirectly, data protection and marketing legislation will apply - even if they are acting in a professional capacity.

For example, if you have the name and number of a business contact on file, or their email address identifies them (e.g. initials.lastname@company.com), the legislation will apply.

# Lawful Basis for Direct Marketing

As with any form of processing of Personal Confidential Information, The **Practice** must ensure that there is an appropriate lawful basis for its direct marketing activities.

In many cases, this will be:

* The individual has consented to receiving direct marketing (Article 6 1 (a)[[1]](#footnote-1)
* The direct marketing is necessary for the legitimate interests of the Controller (Article 6 1 (f)

**Practice** staff members undertaking or making decisions is relation to direct marketing should consult the Processing Activities Log maintained by the Data Protection Officer to ensure that are aware of the legal basis and the limitations or rules concerned.

# Opt in / Out Out

The implementation of the updated data protection legislation and increased threshold for obtaining consent requires organisations to consider whether it is necessary to obtain ‘fresh’ consents for their marketing activities.

This depends on the lawful basis. Where the lawful basis is consent and the original approach to consent meets the legal threshold, it will not be necessary to re-opt in. A template is available at Appendix A to assist with this determination.

Where the lawful basis is ‘legitimate interests’, consent is not required.

Recital 47 provides that ‘The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest’[[2]](#footnote-2).

For this to be an appropriate lawful basis:

* There must be a relevant and appropriate relationship between the data subject (such as the data subject being a client of the organisation)
* The organisation has determined that the individual ‘reasonably expects’, at the time and context of when the data was collected, that it would be used in such a way
* Where it is not clear whether the individual would reasonably expect such a use, there should be careful consideration of the rights and freedoms of the individual

Ultimately,  **The Practice** may determine that sending marketing to its existing customer basis is appropriate on legitimate interest ground without obtaining consent, however, they must always be offered an opportunity to opt out of such contact.

# Texting Patients

The majority of direct marketing for practice will be texting patients to make them aware of appointments or services of interest.

The DPO has assessed this activity and concluded that, rather than “consent”, the appropriate legal gateway for this activity is “legitimate interests”.

This means that the activity is necessary for the practice to undertake their duties as a healthcare provider – see Appendix B.

In order to maintain the lawfulness of this approach the following actions must be completed by the practice;

* It should be made clear within the registration documents that mobile numbers will be used for this type of communication
* Communication preferences should be regularly checked with patients
* Patients must be provided with an opportunity to opt out (if the technology allows, this should be within the text, if not, there should be posters displayed in the physical premises providing options to change their preferences)

# Associated Protocols

This policy should be read in conjunction with:

* Risk Management Policy
* Change Management Policy
* Information Governance Policy
* Information Rights and Access Protocol
* Information Sharing and Privacy Protocol
* Information Lifecycle and Data Quality Protocol
* Information / Cyber Security Protocol
* Information Incident Protocol
* Information Risk and Audit Protocol
* Data Protection Impact Assessment Protocol
* Freedom of Information Protocol

# Audit Schedule

Direct Marketing will be audited through the Information Governance Audit provided in the Information Risk and Audit Protocol.

# Review

This protocol will be reviewed every year or sooner where necessary.

# Appendix A

**Consent Checklist**

This checklist draws from the Information Commissioner’s Office GDPR At a Glance Checklist[[3]](#footnote-3) and supports **Practice** staff to determine whether consent is appropriate and valid as a legal basis for processing of personal data.

Where one of the criterion cannot be satisfied and evidenced, valid consent is not being obtained and an alternative lawful basis should be considered.

|  |  |
| --- | --- |
| **Name of Processing Activity (i.e. hospital referral)** |  |
| **Completed by** |  |
| **Date** |  |

|  |  |  |
| --- | --- | --- |
| Valid Consent Criterion | Detail | Status |
| We have made the request for consent prominent and separate from our terms and conditions | *Example: We provide a clear tick box specifically for direct marketing purposes* |  |
| We ask people to positively opt in. | *Example: individuals are required to ask to use tick box to say they are happy for information to be used this way.* |  |
| We don’t use pre-ticked boxes or any other type of default consent. | *Example: individuals are required to complete a consent form and tick to say they are happy for information to be used in this way.* |  |
| We use clear, plain language that is easy to understand. | *Example: Fair Processing materials are available in Easy Read, pictorial and video form as well as written text. Other languages are available.* |  |
| We specify why we want the data and what we’re going to do with it. | *Example: individuals are provided with a list of specific activities we undertake using their data* |  |
| We give individual (‘granular’) options to consent separately to different purposes and types of processing. | *Example: individuals are able to indicate what activities they are happy for us to use their data for and which they aren’t. This can be recorded in local systems.* |  |
| We name our organisation and any third-party controllers who will be relying on the consent. | *Example: Our privacy notices list all of our sharing partners specifically by name.* |  |
| We tell individuals they can withdraw their consent. | *Example: contact details are provided for individuals to withdraw consent from any or all of the processing activities.* |  |
| We ensure that individuals can refuse to consent without detriment. | *Example: Withdrawal of consent to marketing does not affect the individual’s ability to access our services* |  |
| We avoid making consent a precondition of a service. | *Example: Withdrawal of consent to marketing does not affect the individual’s ability to access our services* |  |
| If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place. | *Example: We deliver a health app that children can access. Age is verified through biometric authentication.* |  |
| We keep a record of when and how we got consent from the individual. | *Example: Our system allows us to record when consent was obtained and upload consent forms.* |  |
| We keep a record of exactly what they were told at the time. | *Example: The privacy information is version controlled. When a change is made to information flows, consent is obtained again by re-providing the privacy notice.* |  |
| We regularly review consents to check that the relationship, the processing and the purposes have not changed. | *Example: Quarterly reviews of consents are undertaken to ensure that consent remains valid.* |  |
| We have processes in place to refresh consent at appropriate intervals, including any parental consents. | *Example: Quarterly reviews of consents are undertaken to ensure that consent remains valid.* |  |
| We consider using privacy dashboards or other preference-management tools as a matter of good practice. | *Example: Our system allows us to record granular levels of consent and to give effect to them through read codes.* |  |
| We make it easy for individuals to withdraw their consent at any time and publicise how to do so. | *Example: Our staff are trained to action withdrawal of consent and the option is also available on our website.* |  |
| We act on withdrawals of consent as soon as we can. | *Example: Our staff are trained to action withdrawal of consent and the option is also available on our website.* |  |
| We don’t penalise individuals who wish to withdraw consent | *Example: Withdrawal of consent does not affect the individual’s ability to access services.* |  |

# Appendix B Texting Patients about Appointments and Services (GDPR Recital 47 Legitimate Interests Assessment)

The practice uses a texting service to send information to patients about appointments and services and has determined that the processing of personal data in this way is lawful by virtue of Article 6 (f) GDPR;

“processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child”

Satisfaction of this lawful basis requires “careful assessment” to ensure that the legitimate interests of practice are not overridden by the rights and freedoms of the data subjects concerned.

Data Protection law requires consideration of several factors and each are considered under the headings below.

**What are the legitimate interests of the Controller?**

The practice seeks to fulfil its statutory duties under the Health and Social Care Act 2012 to promote and deliver health services to citizens. Communication with patients about services and appointments serves this function and facilitates the care of the data subject.

**What are the Reasonable Expectations of the Data Subject?**

Individuals provide their mobile phone details as part of their registration and the registration documents make it clear that this kind of communication (text alerts) will be used.

These kinds of updates were previously made by telephone or letter. It is acknowledged that texts are potentially more privacy intrusive (since they do not provide the option not to receive the message – such as through not answering the phone) however, it is important that the practice use modern technology to ensure the most effective route to communicate with patient population.

The practice recognises, however, that when there is a less intrusive method of communication available, it is necessary to provide data subjects with an opportunity to “opt out” of text messages and use traditional routes.

The Direct Marketing Protocol advises that;

* It should be made clear within the registration documents that mobile numbers will be used for this type of communication
* Communication preferences should be regularly checked with patients
* Patients must be provided with an opportunity to opt out (if the technology allows, this should be within the text, if not, there should be posters displayed in the physical premises providing options to change their preferences)

**What Impact Does the Activity Have on the Rights of the Individual?**

Through the measures above, the individual retains the ability to indicate that they would rather not receive the alerts in the first place as well as alter their sharing preferences. The individual is informed of the presence of text alerts both at registration and within the practice privacy materials, through which they are made aware of the right to object, right to access / restriction and complain.

Individuals have a right to privacy and this is maintained as much as practicable through Ensuring that the texts are only used in relation to health care services.

**Conclusion**

It is therefore concluded that the rights and freedoms are not disproportionately interfered with and that, where possible the practice have employed measures to maintain those rights and freedoms.

It is determined that, given the measures above, the practice has satisfied the criteria for establishing the lawful basis of Article 6 (f) GDPR.

1. General Data Protection Regulations 2016/679 (GDPR) [↑](#footnote-ref-1)
2. http://www.privacy-regulation.eu/en/r47.htm [↑](#footnote-ref-2)
3. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [↑](#footnote-ref-3)