Terms and conditions

Please read these terms of use carefully. By downloading this COVID-19 NI Contact Tracing App you agree to these terms.

Introduction

These are the terms of use for the COVID-19 NI Proximity App (also referred to as StopCOVID NI) which is being made available by the Department of Health (DoH) in Northern Ireland (under powers available through the 'Health and Social Care (Reform) Act (Northern Ireland) 2009'). The App has been designed to assist in stopping the spread of COVID-19 in Northern Ireland, by anonymously contacting people who have been in close contact with someone who has tested positive for COVID-19. The App has been developed on behalf of the DoH for the benefit of citizens in Northern Ireland.

The phones of those who are using the App emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, App users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time, both will store the anonymous 'key' of the other phone for 14 days.

'Authorisation Codes' are anonymous random six digit alphanumeric codes generated to verify that a positive test has been received by the App user, allowing 'exposure notifications' to be sent via the App, when the user enters a valid 'authorisation code.' On entering the code, the user is asked to release the anonymous keys their phone has transmitted over the previous 14 days: these are then known as 'diagnosis keys'. These are then released to the secure registry supporting users of the App, to be shared with other App users.

'Diagnosis keys' are anonymised identifiers generated on entry of an 'authorisation code' on the App, and stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London). Every App user's phone regularly checks for 'diagnosis keys' and where these match a significant contact episode's anonymous 'key' stored on their phone, over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the App user's phone, not in the secure registry.

Where 'Exposure Notification' is mentioned, this refers to an anonymous notification, received via the App, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected.

Please read these terms of use in conjunction with the Privacy Information Notice for the App, available to view below.

References to "DoH", "we" and "us" in these terms of use are to the Department of Health NI which is the owner and licensor of the StopCOVID NI Contact Tracing App. References to "the user" and "you" refer to the person who has downloaded the App onto their device for their own personal use and who uses the service.

What the StopCOVID NI Contact Tracing App does

The StopCOVID NI Contact Tracing App only provides one function, namely 'exposure notification'. It is a clearly declared position that no further functions will be added to this App, and that use of GPS location functionality will **NOT** be added at any time by the DoH.

Exposure Notification

The App records if users are in close contact with another App user (see above). If an App user tests positive for COVID-19 the App will notify any App users that have been closer than two metres for more than fifteen minutes (this is in line with current public health policy, and can be changed depending on advised best practice), in the previous 14 days. The App uses capabilities of mobile operating systems. Apple and Google have developed a method that allows specific government-only COVID-19 Apps to make use of Bluetooth technology on phones that would otherwise not be available. As the App will need to use the most current version of the phone's operating system, users may be asked to upgrade the first time they use it. None of the information in this App is ever shared with Apple or Google. The App cannot be used on older phones, on which it is not possible to upgrade the operating system. It is not available on phones which use a different operating system, other than the Android or iOS systems deployed by Google / Apple.

First time use

The first time anyone uses the App they are prompted to allow the App to collect and share the anonymous data transmitted by nearby devices that also have the App installed.

Metrics Data

Metric data does not identify you and is used to create aggregate views of how the App is being used and the impact it is having on the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation.

1. The total number of App users
2. The total number of instances where 'diagnosis keys' have been uploaded
3. The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period.

If you are notified that you have been in close contact with someone who has tested positive, you will be advised to self-isolate for 14 days. If you have symptoms you will be directed to check your symptoms at https://covid-19.hscni.net/ (where you can download the 'COVIDcare NI' symptom checker App if you do not already have it) and book a test.

Use of the StopCOVID NI Contact Tracing App.

The StopCOVID NI Contact Tracing App is free to download and use to anyone who is resident in Northern Ireland. The Service is intended only for people resident in Northern Ireland and the Service may not be otherwise used.

Users downloading the App who are not resident in Northern Ireland will not be able to receive authorisation codes, in relation to a positive test for COVID-19, as the app is linked to the NI test registry (which only receives results in relation to people resident in Northern Ireland). On downloading and activating the App, users are asked to confirm that they are resident in Northern Ireland and, if not, are discouraged from using the App with an explanation that it will not work for them. They are encouraged to use an App intended to cover their own area.

It is intended that the StopCOVID NI Contact Tracing App will be able to be used by those resident in Northern Ireland visiting anywhere in the Republic of Ireland; and it is intended that those using the App launched in the Republic of Ireland may use that App when visiting Northern Ireland. This will be achieved by delivering 'interoperability'. 'Interoperability' is achieved by the secure sharing of anonymous 'diagnosis keys' on a secure shared 'federated server' hosted on the Dublin AWS account of the DoH IRL. The server is only accessible to the apps of app users, and is not otherwise accessible. The server only contains non-identifiable data, 'diagnosis keys stripped of any indefinable information, and as such falls out with the scope of GDPR. This is governed by a bilateral agreement between the Departments of Health in both countries, a MOU. It is not accessible by any other means other than the Apps of the two countries. It is intended that as other countries release similar Apps, more agreements will be reached to share anonymous 'diagnosis keys', enabling users of the StopCOVID NI app to use the app visiting other countries. These 'keys' cannot be used to identify any individual, and are totally anonymous. The ability for App users who travel to be able to receive notifications, and enable others to receive notifications if they test positive is important to help stop spread of COVID as people start to travel again.

Use of the App requires an Android or iPhone mobile telephone device which supports Android 6.0 or higher (in the case of Android phones) or iOS 13.5 or later (in the case of iPhones). In addition, in order to operate correctly, the App also requires Bluetooth functionally turned on and the COVID Exposure Notification service enabled.

If you consent to the Exposure Notification service provided by the App and want to receive those services, you will need to enable Bluetooth and location services and you will need to permit push notifications from the App. The App will prompt you about enabling these services and providing permissions if and when you give your consent to receive the service from the App. The App does not use GPS location services, or Google location services to track your movements. The App simply uses the strength of the Bluetooth signal of phones, with the App activated, to measure the proximity of those phones, and the length of time spent at a given proximity.

More about the DoH and the licence to use the App

We license you to use:

The Covid-19 Contact Tracing mobile application software and the data supplied with the software (the StopCOVID NI Contact Tracing App) and any authorised updates or supplements to it;

The related online or electronic documentation related to the App (Documentation), and The Services you connect to via the App and the content we provide to you through it, as outlined above, subject to and as permitted in these terms.

The above licence is a personal, non-exclusive, non-transferable, revocable, limited licence to use the StopCOVID NI Contact Tracing App and the Documentation, and through the App to use the Services, for your own personal use. All other licence rights not expressly permitted are fully reserved to us.

If you want to report back to us about your experience of using the StopCOVID NI Contact Tracing App, or want to report any problems with the use of the App or the Services, please contact us by calling '**0300 200 7896**' and selecting the option to speak to someone to log a request, at the following times; Monday-Friday (excluding bank

holidays) between the hours of 8:30am – 5:30 pm. You will also find more information at https://covid-19.hscni.net/

Your Privacy

We only use any data we collect through your use of the App and the Services in the ways set out in our Privacy Information Notice. The Privacy Information Notice confirms the terms upon which your data is collected and used in respect of your use of the App and the Services.

App Store's terms also apply

When you download the App, or when you access or use the App or the Services, you may also be subject to the terms of use and policies of the relevant App Store (Google Play Store or Apple Store) from which you download the App. Please review these terms of use and policies very carefully. Your access to, and use of, the Services will be governed by these (the DoH's) terms of use, unless the terms of use and policies of the relevant App Store say otherwise.

How you may use the App, including how many devices you may use it on

In return for your agreeing to comply with these terms you may:

- download a copy of the App onto one mobile device and view, use and display the App and the Services on this device for your personal purposes only,
- use any Documentation to support your permitted use of the App and the Services,
- provided you comply with the licence restrictions above, make one copy of the App and the Documentation for back-up purposes, and
- receive and use any free supplementary software code or update of the App incorporating "patches" and corrections of errors as we may provide to you.

You must be 18 to accept these terms and to download and use the App

You must be at least 18 years of age in order to accept these terms and to download and use the App.

The right to use the App and Services is personal and you may not transfer the App to someone else

We are giving you personally the right to use the App and the Services as set out above. The use of the App by multiple individuals from the same device undermines the accuracy and efficacy or the App's contact tracing function (if enabled). If you permit someone else to access your device and to use the App or Services, then you do so at your own risk, and you are responsible for that person's use and you must ensure that the person knows about and complies with these terms. You must also not use any other person's StopCOVID NI Contact Tracing App.

You may not otherwise transfer the App or the Services to someone else, whether for money, for anything else or for free. If you sell any device on which the App is installed, you must first remove the App from the device.

Changes to these terms

We may need to change these terms to reflect changes in law or best practice or to deal with additional features which we introduce.

We will give you at least 7 days' notice of any change by sending you an in-App notification and providing you with details of the change, on this publication, and notifying you of a change when you next start the App.

Changes driven

Northern Ireland Public health policy may not be subject to the 7 days' notice, as the timing of implementation may not allow it. We will publicly notify changes in the app and on https://covid-19.hscni.net/stop-covid-ni-mobile-app in advance.

If you do not accept the notified changes, we will advise you what specifically this will mean at the date of the notification. It may mean that you will not be permitted to continue to use the App and the Services. This will be your informed choice.

Updates to the App and changes to the Services

From time to time we may automatically update the App and change the Service settings to improve performance, enhance functionality, reflect changes to the operating system or address security issues. Alternatively, we may ask you to update the App for these reasons. If you choose not to install such updates or if you opt out of automatic updates you may not be able to continue using the App and the Service, and you may compromise the security of your data or device.

If someone else owns the phone or device you are using

If you download or stream the App onto any phone or other device not owned by you, you must have the owner's permission to do so. You will be responsible for complying with these terms, whether or not you own the phone or other device.

We are not responsible for other websites you link to

The App or any Service may contain links to other independent websites which are not provided by us, such as websites for purposes of booking a test. Such independent sites are not under our control, and we are not responsible for and have not checked and approved their content or their privacy policies (if any). You will need to make your own independent judgement about whether to use any such independent sites.

Licence restrictions

You agree that you will:

- except in the course of permitted sharing, see information on how you may use the app above, not rent, lease, sub-license, loan, provide, or otherwise make available, the App or the Service in any form, in whole or in part to any person without prior written consent from us, nor will you infringe our rights (including our intellectual property rights) in relation to your use of the App or Services;

- not copy the App, Documentation or Services, except as part of the normal use of the App or where it is necessary for the purpose of back-up or operational security;
- not translate, merge, adapt, vary, alter or modify, the whole or any part of the App, Documentation or Services nor permit the App or the Services or any part of them to be combined with, or become incorporated in, any other programs, except as necessary to use the App and the Services on devices as permitted in these terms;
- not disassemble, de-compile, reverse engineer or create derivative works based on the whole or any part of the App or the Services nor attempt to do any such things, except to the extent that (by virtue of 'The Copyright (Computer Programs) Regulations 1992') such actions cannot be prohibited because they are necessary to decompile the App to obtain the information necessary to create an independent program that can be operated with the App or with another program (Permitted Objective), and
- provided that the information obtained by you during such activities is not disclosed or communicated without our prior written consent to any third party to whom it is not necessary to disclose or communicate it in order to achieve the Permitted Objective, is not used to create any software that is substantially similar in its expression to the App, kept secure; and is used only for the Permitted Objective,
- comply with all applicable technology control or export laws and regulations that apply to the technology used or supported by the App or any Services.

You must:

- ensure that all information that you provide to us via the App is accurate, complete, honest and not misleading, to the best of your knowledge, information and belief;
- comply with all applicable laws and regulations in using the App and the Services;
- not use the App or any Service in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these terms, or act fraudulently or maliciously, for example, by hacking into or inserting malicious code, such as viruses, or harmful data, into the App, any Service or any operating system;
- not infringe our intellectual property rights or those of any third party in relation to your use of the App or any Service, including by the submission of any material (to the extent that such use is not licensed by these terms);
- not transmit any material that is defamatory, offensive or otherwise objectionable in relation to your use of the App or any Service;
- not use the App or any Service in a way that could damage, disable, overburden, impair or compromise our systems or security or interfere with other users; and
- not collect or harvest any information or data from any Service or our systems or attempt to decipher any transmissions to or from the servers running any Service.

Intellectual property rights

All intellectual property rights in the App, the Documentation and the Services throughout the world belong to us and the rights in the App and the Services are licensed (not sold) to you. You have no intellectual property rights in, or to, the App, the Documentation or the Services other than the right to use them in accordance with these terms.

Our responsibility to you

No warranty. While we take every care to ensure the correctness of the information, content and communications published in the app, we make no representation, warranty or guarantee as to the correctness, accuracy, completeness, currency or reliability thereof. We assume no responsibility and make no warranty that the functions and use of the App will be permanently and continuously available and free of errors or faults, that errors will be rectified, or that the App will be free of viruses or other harmful elements.

Exclusion of liability. To the extent permitted by law, any claims for liability against us due to material or immaterial damage, including indirect or consequential damage, arising for example from access to, use or non-use of the App and the associated information, content and communications, from misuse of the connection or technical faults or any other loss or damage whether arising under tort (including negligence), breach of contract, breach of statutory duty or otherwise, are hereby excluded.

We do not exclude or limit in any way our liability to you where it would be unlawful to do so. This includes liability for death or personal injury caused by our negligence or the negligence of our employees, agents or subcontractors or for fraud or fraudulent misrepresentation, or in respect of any of your legal rights as a consumer (to the extent that these cannot be excluded).

Limitations to the App and the Services. While the App provides notification to those who may have been exposed to a confirmed positive case, providing advice to self-isolate, the App provides no additional functions. All those in Northern Ireland with a positive test result for COVID-19 would be expected to receive a phone call from a clinical professional employed on the Test Trace and Protect programme. This public health service, provided in Northern Ireland, is separate from the App and works in parallel. The App works in an anonymous and automated way, in parallel to the manual Test Trace and Protect contact tracing process. Information from the app is not shared with those working in the manual service.

Automated processing. The generation of exposure notices on the app is an automated process, not involving a human. The automated process is carried out by use of anonymous identification keys, and measurement of Bluetooth signals to calculate that App users' phones have been close enough for long enough to constitute a significant contact, sufficient to put you at risk of having been infected. It is necessary for the app to do this in an automated way, in order to protect your identity and the identity of other app users. In accepting terms and conditions you are consenting to this process. If you need to discuss this with an individual, you can call '**0300 200 7896'** Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. **App users can express their point of view and contest the decision.**

Withdrawal of or changes to the App or Services. The App and Services are intended to be made available for a limited period only while the Covid-19 crisis is ongoing. Without prejudice to this, we expressly reserve the right, at any time, without prior notice, to withdraw the App and Services. We also expressly reserve the right, at any time, and without prior notice, to make changes and/or improvements to the App and Services.

Please back-up content and data used with the App. We recommend that you back up any content and data used in connection with the App, to protect yourself in case of problems with the App or the Service.

Check that the App and the Services are suitable for you. The App and the Services have not been developed to meet your individual requirements. Please check that the facilities and functions of the App and the Services (as described on the App Store site and in the Documentation) meet your requirements.

We are not responsible for events outside our control. If our provision of the Services or support for the App or the Services is delayed by an event outside our control then we will contact you as soon as possible to let you know and we will take steps to minimise the effect of the delay. We will not be liable for delays caused by the event, but if there is a risk of substantial delay you may contact us to end your use of the App at any time.

You can end your use of the App and what happens if you do

You can stop using the App at any time, and you can delete it at any time from your device.

If you delete the App, you will not be able to access the Services, and all rights granted to you by these terms will cease. We will not be holding any personal data in relation to you, since we will not be collecting any; however any data held on your phone can be removed as indicated in the App instructions. Details are provided in relation to data processed by the App in the Privacy Information Notice.

We may end your rights to use the App and the Services if you break these terms

We may end your rights to use the App and Services at any time by contacting you if you have broken these terms in a serious way. If what you have done can be remedied we will give you a reasonable opportunity to do so.

If we end your rights to use the App and Services:

- You must stop all activities authorised by these terms, including your use of the App and any Services.
- You must delete or remove the App from your device(s) and immediately destroy all copies of the App which you have and confirm to us that you have done this.
- We may end support and linkage to the App, form the App backend, rendering the App redundant.

We may transfer our rights and obligations to someone else

We may transfer our rights and obligations under these terms to another organisation. We will always tell you in writing if this happens and we will ensure that the transfer will not affect your rights under the terms of the licence.

You need our consent to transfer your rights to someone else

You may only transfer your rights or your obligations under these terms to another person if we agree in writing.

No rights for third parties

In respect of any individual not resident in Northern Ireland downloading and using the App: it is clearly our stated intent, that this app should **not be used by individuals who are not resident in Northern Ireland**. In order to avail of the App's functionality in terms of exposure notification, it is essential that users are resident in Norther Ireland, in order for us to be able to deliver authorisation codes in relation to their test results. During the on-boarding process, App users are given clear instruction not to use the App if they are not resident in Northern Ireland, and that the App functionality will not be available to them. As a result, we can accept no liability for anyone ignoring the instruction and using the App improperly.

If a court finds part of these terms illegal, the rest will continue in force

Each of the paragraphs of these terms operates separately. If any court or relevant authority decides that any of them are unlawful, the remaining paragraphs will remain in full force and effect.

Even if we delay in enforcing these terms, we can still enforce them later

Even if we delay in enforcing these terms, we can still enforce them later. If we do not insist immediately that you do anything you are required to do under these terms, or if we delay in taking steps against you in respect of your breaching these terms, that will not mean that you do not have to do those things and it will not prevent us taking steps against you at a later date.

Terms survive

Any of these terms of use that are intended to come into or continue in force on or after termination or expiry of these terms (which includes for the avoidance of doubt the provisions dealing with *Our responsibility to you*) will remain in full force and effect following termination or expiry. Termination or expiry of these terms of use shall not affect any rights, remedies, obligations or liabilities of you or us that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the terms of use which existed at or before the date of termination or expiry.

Which laws apply to these terms and where you can bring legal proceedings

These terms are governed by the law of Northern Ireland and you can bring legal proceedings in respect of these terms (or anything to do with the App or the Services) in the courts in Northern Ireland only.

Privacy Information

Data Controller Contact Details

Department of Health (DoH)
Castle Buildings
Stormont
Belfast
BT4 3SG

Contact- Chief Digital Information Officer Group

CDIO@health-ni.gov.uk

Data Protection Officer

Charlene McQuillan

DPO@health-ni.gov.uk

Introduction

The purpose of this information notice is to explain how the StopCOVID NI Contact Tracing App works, what data is collected by the app, and who has access to that data and the purposes for which they use it.

Use of the app is entirely voluntary and is available to download for free from the Apple App Store and the Google Play Store. The app runs on iPhones that support iOS 13.5 and higher, and Android phones running Android 6.0 and higher. The App is not intended for use by persons under 18 years of age, at present, as anonymity to protect App users (in line with GDPR) creates a conflict with safeguarding issues, and the requirement for parental consent. You will be asked to confirm that you are 18 years or older when you download the App. The App is only intended for use by individuals resident in Northern Ireland. You will be asked to confirm residency and will be discouraged from using the App if you do not meet this criteria. We accept no liability for improper use, outside these defined conditions.

The Data Controller

The Department of Health (DoH) in Northern Ireland is the Data Controller – it has decided the means and purposes for the processing of data collected and used by the app. The DoH, working with the Health and Social Care Board and Public Health Agency (PHA), has commissioned all app related systems for processing all data. The DoH provides strategic direction for the app.

The DoH is therefore responsible for your personal data and has determined its responsibilities for compliance with its obligations under data protection laws. The DoH has provided access to speak to someone via '**0300 200 7896**' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm, should you wish to raise an issue in relation to how your data is managed by the App, though note that you also have the right to contact the Data Protection Officer in this regard.

What the app does

The purpose of the app is to support the public health response to the COVID-19 crisis in Northern Ireland. The app has the following functions:

1. Exposure Notification – the App, through use of anonymous 'keys', records when App users' phones have been in proximity to each other, for a sufficient period of time to mean that it is possible that the coronavirus has been passed on. Should an App user test positive for COVID-19, it is possible for them to alert other App users anonymously via the functions supported by the App.
2. Registering a Positive Test Result – App users who have a positive test for COVID-19 will receive a randomly generated 'authorisation code' via SMS text message. This process is managed via a separate test registry, administered by the Regional Business Services Organisation (in accordance with its statutory functions as defined in the Health and Social Care (Reform) Act (Northern Ireland) 2009). This is separate from the App, in order to keep personal and identifiable information separate from the APP.
3. Other Functions – the app will collect Metric data which do not identify you in order to create aggregate views of how the App is being used and the impact it is having on controlling the spread of the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation:

    a. The total number of App users
    b. The total number of instances where 'diagnosis keys' have been uploaded
    c. The total number of 'exposure notifications' triggered

    The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period. **As a precaution, in information governance terms, we treat the metrics as 'health data' to ensure your information is protected in terms of GDPR legislation.**

You are not requested to enter any personally identifiable information on the App. The 'App settings' give you the ability to delete the App and any information stored on the phone while using the App. The information collected is essential in allowing the App to meet its obligations for formal approval as a medical device and CE accreditation; in line with requirements published by the Regulator, MHRA. The regulator, in line with stated policy for the period of the COVID-19 pandemic, has granted a 6 month approval of the App for use, until formal permanent accreditation is obtained. Appropriate interim assurance on reliability and effectiveness has been provided to the regulator. Your explicit consent is obtained during the on-boarding process in order to enable the release of the diagnosis keys and to enable decisions to be taken on an automated basis. Collection of the metric data is essential for the DoH meet its regulated obligations in relation to CE accreditation, and to allow the DoH to support the essential public health function of contact tracing in delivering infection control measures in the context of the COVID-19 pandemic.

The phones of those who are using the App emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, App users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time (currently defined as 2 metres or less, and a duration of 15 minutes or more), both will store the anonymous 'key' of the other phone for 14 days.

'Authorisation Codes' are anonymous random six digit alphanumeric codes generated to verify that a positive test has been received by the App user, allowing 'exposure notifications' to be sent via the App, when the user enters a

valid 'authorisation code.' On entering the code, the user is asked to release the anonymous keys their phone has transmitted over the previous 14 days: these are then known as 'diagnosis keys'. These are then released to the secure registry, (see details below - HSCB AWS account), supporting users of the App, to be shared with other App users.

'Diagnosis keys' are anonymised identifiers generated on entry of an 'authorisation code' on the App, and stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London). Every App user's phone regularly checks for 'diagnosis keys' and where these match a significant contact episode's anonymous 'key' stored on their phone, over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the App user's phone, not in the secure registry.

Where 'Exposure Notification' (ENS) is mentioned, this refers to an anonymous notification received, via the App, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected.

The DoH is content to give a firm assurance that it has no intention to add to the functions of the StopCOVID NI App, beyond those identified above.

Future updates of the App may occur to improve the performance of existing functions, or to implement improvements in the Google-Apple operating system that may occur to improve performance, within the scope of existing functions (outlined above). The DoH is considering the future development of versions of the App, to address accessibility in terms of languages other than English. This decision will be balanced against public health benefit and cost (balanced against other health priorities).

How the app works

Let's look at each feature in the app in detail.

How Contact Tracing works

Existing manual contact tracing processes rely on you being able to remember who you have been in contact with recently, and for how long. In many cases you may not even know those people (for example, if the contact happened on a bus or train, at a concert, a restaurant or some other public venue).

The app uses technology developed by Apple and Google where anonymous rolling identifiers are exchanged between mobile phones. A random and unique identifier is generated by your phone every 15 minutes (range - 10 to 20 minutes). If you are close to someone, who also uses the app on their phone, your identifier will be saved on that person's phone and you will record their identifier on your phone. All identifiers collected will remain on your mobile but you can't see them, nor can anyone else. These anonymous identifiers cannot identify you, to other users, or to the DoH.

If a person using the App subsequently receives a positive COVID-19 diagnosis, they will receive a text message containing an 'authorisation code' via SMS. The Business Services Organisation test registry generates a test notification to all those who have a registered mobile phone number on their records, or who have registered for testing via the website https://www.nhs.uk/ask-for-a-coronavirus-test. The Business Services Organisation does not know who is using the App, so notifications are sent to in relation to all positive tests, where mobile phone numbers have been registered to testing services or for receipt of medical services in NI. All those with a positive

test will also receive a phone call from a clinical professional as part of the 'Test Trace and Protect' programme, administered by the Public Health Agency (PHA) under powers available through the 'Health and Social Care (Reform) Act (Northern Ireland) 2009'. On the call, they will be asked if they are using the StopCOVID NI Contact Tracing App and if yes, if they have not already done so, if they wish to enter an 'authorisation code' to the app to enable the upload of 'diagnosis keys' from their phone. To do this, the PHA will send them a code by SMS, which when entered into the app unlocks an upload function. The person makes a choice to upload 'authorisation code' and release 'diagnosis keys' relating to the anonymised identifiers of significant contacts processed on their own phone, to a secure registry maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services based in London; where the 'diagnosis key' identifiers are published to be visible to other App users phones, enabling 'Exposure Notifications'. The SMS text message is delivered using the Gov.UK Notify service https://www.notifications.service.gov.uk/ .

Every two hours, the latest 'Diagnosis Keys' from the App Registry will be downloaded by every user's phone. These will be used to check for matches against the identifiers of the contacts that have been collected by your phone. If there is a match, you will be notified in the app that you were in close contact with a person who was diagnosed with COVID-19; this is called an 'Exposure Notification'.

For all this to work, you have to allow 'COVID-19 Exposure Notification Services' on your phone. You can also choose to allow your phone to display notifications so that you also receive an alert on your phone that you have been exposed to someone who has tested positive for COVID-19. You can turn off this functionality, if you change your mind, in the settings page of the app.

It is important to note that Contact Tracing never reveals the identity of any person using the app to other app users, and never reveals who has been diagnosed positive. Also, the PHA and DoH will not know if you receive an 'exposure notification'.

Automated processing. The generation of exposure notices on the app is an automated process, not involving a human. The automated process is carried out by use of anonymous identification keys, and measurement of Bluetooth signals to calculate that App users' phones have been close enough for long enough to constitute a significant contact, sufficient to put you at risk of having been infected. It is necessary for the app to do this in an automated way, in order to protect your identity and the identity of other app users. In accepting terms and conditions you are consenting to this process. If you need to discuss this with an individual, you can call '**0300 200 7896**' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. **App users can express their point of view and contest the decision.**

What App metrics are collected

1. Collected regionally

The app will collect Metric data, which does not identify you, to create aggregate views of how the App is being used and the impact it is having on the control of the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation:

1. The total number of App users
2. The total number of instances where 'diagnosis keys' have been uploaded
3. The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period.

2. Generated by services on the phone

The following data is generated by Exposure Notification Services running on your phone if you turn it on.

1. Identifiers sent and received between phones that have ENS turned on.
2. Identifiers (diagnosis keys) uploaded to the Health & Social Care Board (HSCB) secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London) (AWS) Registry if you are COVID-19 positive and you agree to upload them.
3. Identifiers (diagnosis keys) downloaded from the AWS Registry to your phone for matching.

The above identifiers are random alpha numeric values that cannot be used to identify you or anyone else. These are generated, collected and matched on your phone if you enable ENS.

3. Automatically collected from your phone:

As a consequence of how traffic passes across the Internet, your internet protocol (IP) address is also inevitably transferred to our network servers. An IP address is typically made up of 4 sets of numbers (e.g. 1.2.3.4) and is assigned to you by your mobile phone or Wi-Fi service provider. Under the GDPR your IP address is regarded as your personal data.

While your data travels with the IP address it is considered personal data. The DoH does not use your IP address to identify you; furthermore the IP address is removed and deleted at the 'font door' of the HSCB AWS account, and the information becomes anonymous again and cannot be linked back to you. We do **not** store the IP addresses.

The legal basis for data processing

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 together form a framework for regulating the processing of personal data in the UK from 25th May 2018.

In relation to 'Metrics' and 'IP address and app security tokens' the '**processing is necessary for the performance of a task carried out in the public interest**' as per GDPR Article 6(1)(e). The legal basis for the data processing is The Health and Social Care (Reform) Act (Northern Ireland) 2009,

- Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and
- Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and
- Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

In relation to Special Category data, Article 9(2)(i) applies to the processing, '**processing is necessary for reasons of public interest in the area of public health**'. Under DPA 2018, Schedule 1, Part 1 condition 3 is met in relation to Article 9 as follows:

Public health

3 .This condition is met if the processing—

a) is necessary for reasons of public interest in the area of public health, and
b) is carried out—
    i. by or under the responsibility of a health professional, or
    ii. by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

The app cannot function beyond the initial 6 month MHRA Exemption from device regulation during COVID-19 without attaining CE accreditation. The metrics data, collected at a regional level, are essential in demonstrating efficacy (which will be essential for attaining accreditation). The app cannot be used beyond the 6 month exemption without accreditation. A mobile smartphone cannot link via a network to transfer data without use of an IP address and app security tokens. This information is deleted at the earliest opportunity and not stored anywhere in the infrastructure.

The MHRA guidance on medical devices states:

- "The software must meet all of the general essential requirements and the relevant design and construction essential requirements contained in 'annex I' of the directive. This guidance lists those essential requirements that are likely to apply to software and apps."

General Requirement 3 within Annex I of the Medical Devices Directive states:

- "The devices must achieve the performances intended by the manufacturer and be designed, manufactured and packaged in such a way that they are suitable for one or more of the functions referred to in Article 1(2)(a), as specified by the manufacturer."

'Diagnosis Keys' are released from the phone by the permission of the data subject. They are essential for letting others know that they are at risk of having been infected via the 'exposure notification' process. A person using the app may receive 'exposure notifications' by using the app, utilising the published 'diagnosis keys' of others. They may however decline to enter and 'authorisation code' on receipt of a positive test result, or may decline to release their 'diagnosis keys' for publication. While it is not anticipated that anyone would wish to use the app in such a manner, it is technically the position that release of 'diagnosis keys' is not essential for an app user to consent to this publication process, in order for them to benefit from notification by others. Technically it is arguable that at the point where 'diagnosis keys' exit a user's phone, they are associated with an IP address and app security tokens, and as such are personally identifiable. Though IP addresses vary, and are not static, some more recent rulings have deemed them 'personally identifiable'. Once the IP address and app security tokens have been deleted on entry to the networking layer, the 'diagnosis keys' are non-identifiable. Once stored in the app registry, the 'diagnosis keys' are clearly non-identifiable, and can be published without risk of re-identification. The app is voluntary to use and the legal basis for the processing of the 'diagnosis keys' is 'consent', namely GDPR 6(1) (a), and GDPR 9(2) (a), explicit consent, in relation to the processing of special category data. Consent is sought for release of the 'diagnosis keys' on the app at the point of release.

Security measures

All data stored on your phone is encrypted by the app using the built-in encryption capability of your phone. Data is also encrypted when it is being uploaded to our servers. The App does not store or transmit identifiable information. The App **does not access** GPS functionality on the phone, or access any form of location data from the operating system.

The Contact Tracing feature uses a **fully decentralised** privacy model which means that the matching of identifiers and diagnosis keys happens on your phone and is not externally performed by the DoH. This ensures neither tracking of peoples' movements, nor knowledge of with whom, or when, App users have been in contact with each other.

There is a range of security processes and technologies in place to prevent unauthorised access to the data while it is stored on our servers, including data encryption, modern firewalls and intrusion prevention.

When 'Diagnosis Keys' are uploaded to AWS servers with your IP address, the IP address is stripped from the information at the earliest possible opportunity which renders the information anonymous.

Who processes your data

The DoH has overall responsibility for the app and has directed the Health and Social Care Board (HSCB) and Public Health Agency (PHA) to deliver services in relation to the app, as Data Processors on behalf of DoH. Therefore there are a number of data processors and sub-processors involved in the delivery of the app, who may process data in relation to the app.

Data processors

The following provides a list of data processors and sub processors involved in delivery of the app.

- NearForm are the app developers who will be providing technical support on the running of the app. Their services are delivered via HSCB GDPR compliant contracts.
- Big Motive Ltd are the design team who have worked with NearForm to design the user experience and content for the app.
- Gov.UK Notify provide the service to enable the sending of an SMS to your phone which contains the 'Authorisation Code' needed to enable your phone to release 'Diagnosis Keys'. Their services are delivered via HSCB GDPR compliant contracts. Amazon Web Services provide cloud storage and cloud services for the data uploaded from your phone. Their services are delivered via HSCB GDPR compliant contracts.
- The BSO provide certain services as a data processor on behalf of HSCB and PHA. The BSO host the Covid test registry for lab results. They operate the test registry, gathering the results of testing, positive test results to be notified via SMS text message, and be made available to PHA staff delivering manual contact tracing services, as well as associating results with electronic patient records to ensure appropriate access by clinical professionals supporting clinical care service delivery. They also provide backup support to the SMS function through arrangements with the HSCB. Their services are managed via appropriate agreements with PHA and HSCB.

Contracts and MoUs are in place to govern relationships with the above data processors and sub-processors which set out the obligations of each party and the data controller's obligations and rights with regard to the data that is being processed. All data processing takes place within the EEA area, and as such is subject to legislation in the form of the General Data Protection Regulation (GDPR).

Other recipients

The regional level data (outlined above) is extremely limited in scope. The DoH will make freely available the high level anonymised data, in order for members of the public to see the level of uptake, and the potential of the App to reduce the rate of spread of infection of COVID-19.

Data transferred outside the European Economic Area

No data will be transferred outside the EEA. All data processing will be subject to GDPR regulations and obligations.

How long your personal data is held for

No personal data is collected or stored, but we have outlined below how long certain data connected to the App are retained for.

Your IP Address:

Following upload of your IP address to AWS servers, it is deleted once the server network layer has routed the traffic to the application layer. User IP addresses are never transferred to the application layer.

'Identifier beacons' on your device:

This anonymous information is retained for 14 days.

Diagnosis keys in AWS registry (HSCB account set up on behalf of the DoH):

This anonymous information is retained for 14 days.

Diagnosis keys on your device:

This anonymous information is retained for as long as is necessary to perform a match check and is deleted thereafter.

Gov.UK Notify SMS Service

All SMS texts and phone numbers, processed on the server, are deleted once a SMS text message has been successfully transmitted. This 'server' is physically / electronically separated from the servers supporting the backend of the App. Different service teams will be employed to ensure that identifiable information (mobile phone numbers and test results) are kept separate from the App operational servers, preventing any individuals information being discoverable with the App.

The flow of data from the BSO test registry through the App backend to the Gov.UK Notify (SMS Platform) to send an SMS text will be managed by different groups to help reduce any risk of re identification.

- The BSO registry contains the mobile numbers of people who have tested positive.
- As the Temporary Exposure Key uploads hit the App backend in Amazon Web Services, it is important this backend data cannot be combined with mobile numbers.
- To help prevent this, the Amazon Web Services backend will never store or log the mobile number.
- The mobile number will exist in the BSO test registry and will exist in Gov.UK Notify as SMS messages are sent. (Being deleted after this action has been fulfilled).

To facilitate reconciliation for issues that may occur within the Amazon Web Services backend, a Job ID will be used to track the flow from BSO registry through Amazon Web Services. When BSO calls the Amazon Web Services REST API it will pass on a Job ID that will be used to uniquely identify the transaction with the Amazon Web Services flow.

This Job ID will be logged within Amazon Web Services so that in the case of any failure during processing, the record in the BSO registry that was not successfully processed can be identified.

In the case of a failure during the Amazon Web Services flow, an alert will be raised within Amazon Web Services and notified to the NearForm support team. The NearForm team will investigate alerts raised and will either address or correct, if the issue is within Amazon Web Services.

If the issue is outside of Amazon Web Services, when appropriate, NearForm will escalate the issue to the BSO support team.

BSO will be required to reconcile the Job ID from registry data to the SMS text records on the Gov.UK Notify platform.

The PHA manual Contact Tracing service will also be telephoning all positive test users, so can be scripted to verify that the recipient has received a SMS; the call handler will also have the capability of sending an SMS from the Manual Contact Tracing system.

DoH / HSCB / PHA- Regional Summary Level Information

The DoH / HSCB / PHA will retain regional summary level information, relating to the number of App users / ratio of exposure notifications to positive cases indefinitely, to support evaluation of the App's effectiveness in pursuance of CE accreditation. This process will be conducted in line with requirements outlined by the MHRA, the regulator.

This regional level data will be retained for purposes of research and future pandemic response planning. This does not involve individual data. Though interim approval has been granted, in order to obtain formal MHRA Regulatory approval, and CE certification, will involve collation of data in evidence of the efficacy of the App. In line with GMGR Disposal Schedule J - Clinical Trials of Investigational Medicinal Products (CTIMPs) – this high level summary data will be retained '*for an appropriate period, to allow further analysis by the original or other research teams subject to consent, and to support monitoring by regulatory and other authorities*'. https://www.health-ni.gov.uk/articles/disposal-schedule-section-j

On occasion of the pandemic being declared as having ended, the App will be stood down. Users will be instructed to delete it from their phone. Any anonymised data present, at that time, in the AWS servers (on behalf of the DoH to support the App function) will be deleted.

Data Subject rights

Users have rights under GDPR when their personal data are processed by data controllers. The following considerations should be noted. IP addresses are not retained on the app backend, but for transient network routing and network security purposes. Diagnosis keys are not capable of being associated with a person as they are non-identifying by design.

- **Right to information** – a Data Protection Privacy Notice (Notice) is provided via the app itself on those pages which request information and also in the app Settings. The Privacy Notice will also be published on the DoH website. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

- **Right to rectification** – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for rectification.

- **Right of access** – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for access.

- **Right to erasure** – the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for erasure.

- **Right to restriction** – the user can revoke their ENS permission, revoke their exposure notification permission and decide not to upload keys. Ultimately the user can decide to Leave and/or delete the App from their device. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for restriction.

- **Right to portability** – it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the DoH, the DoH cannot identify which keys belong to which user. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for portability.

- **Right to object** – the user can use the Leave function to delete the information from the app; the user can delete the app from their device and the user can delete ENS data via device settings.

- **Right not to be subject to solely automated decision-making including profiling** – if the ENS detects a match between a Rolling Proximity Identifier on the App and a Diagnosis Key downloaded from DoH Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit informed consent of the user, during the on-boarding process. The automated decision-making is an essential feature of the proximity app solution provided, and is core to nits function in delivering the public health objective of infection control. If App users wish to speak to someone in relation to an 'Exposure Notification' that they have received via the App, they can call '**0300 200 7896**' and select the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. Someone will answer the call and explain the 'Exposure Notification'. They will have no way of knowing with whom, where or

when a 'high risk' contact took place, but they will try to explain the process to App users and its purpose. **App users can express their point of view and contest the decision.** These steps should enable the App user to make an informed decision as to whether to self-isolate to prevent spreading the infection to others. Ultimately if they are still not satisfied or need clinical advice they will be advised to seek clinical assessment by their GP or GP OOH.

Changes to this Data Protection Information Notice

This Data Protection Information Notice may change from time to time and you will receive notification of this update in the app.

How to complain if you are not happy with how we process your personal information

If you are unhappy with any aspect of this privacy notice, or how your personal information is being processed, please contact the Department's Data Protection Officer at the address above.

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113
Email: casework@ico.org.uk

Website: Information Commissioner's Office