

## The Protect Scotland App

### Data Protection Impact Assessment (DPIA)

This document explores, in a transparent way, how the data protection principles and rights of the population in Scotland are observed within the Protect Scotland App; a mobile phone application that is integral part of the Government Test and Protect strategy against the COVID-19 pandemic.



## Data Protection Enquiries

Enquiries should be directed to the App Information Asset Owner (Digital Health and Care Directorate, Scottish Government). Please contact: Digital Health and Care Information Governance Lead [DHCI@gov.scot](mailto:DHCI@gov.scot)

For enquiries directed to The Scottish Government Data Protection Officer, please contact: [DataProtectionOfficer@gov.scot](mailto:DataProtectionOfficer@gov.scot)

For escalation of data protection matters with the Information Commissioner's Office (ICO)

For further information, including independent data protection advice and information in relation to your rights, you can contact the Information Commissioner: Website: [www.ico.org.uk](http://www.ico.org.uk) Tel: 0303 123 1113

You can also report any unresolved concerns here: <https://ico.org.uk/concerns/handling/>.



## Contents

1	The Protect Scotland App.....	3
2	Overview .....	3
3	Roles and Responsibilities .....	6
4	Processing Overview .....	13
4.1	Contact Tracing	15
4.2	Reporting metrics.	23
4.3	Leave function	24
4.4	Management of App settings.	25
4.5	Download and Installation	25
4.6	Exposure Notification Services	26
4.7	Systems involved	27
4.7.1	The Protect-Scot App (Android and IOS) .....	28
4.7.2	The App backend.....	28
4.7.3	Other systems.....	29
4.7.4	Federated interoperability .....	30
4.8	Disclosures of personal data.	31
4.8.1	Other recipients (anonymous data) .....	32
5	Scope of Processing.....	32
5.1	Data Subjects	32
5.2	Personal data	33
5.2.1	Purposes for which personal data is used. ....	37
5.2.2	Data minimisation and anonymisation. ....	38
5.2.3	Data retention.....	40
6	Context of Processing.....	42
6.1	Design Principles	42
6.2	Privacy Model	43
6.3	Children	44
6.4	Novelty and Robustness	47
6.5	Accessibility	48
6.6	Consultation and engagement.	48
6.6.1	Direct engagement with data subjects. ....	50
7	Compliance with data protection legislation and other regulatory guidance .....	53
7.1	Legal basis for the processing.	53
7.1.1	Duty of Confidentiality.....	54
7.1.2	Automated decision-making .....	55
7.1.3	Medical devices regulations. ....	57
7.2	Data Protection rights	58
7.3	Compliance with data protection principles.	60
7.3.1	Principle 1 – fair and lawful, and meeting the conditions for processing .....	61
7.3.2	Principle 2 – Purpose limitation .....	62
7.3.3	Principle 3 – adequacy, relevance and data minimisation .....	62



7.3.4	Principle 4 – accurate, kept up to date, deletion .....	63
7.3.5	Principle 5 – kept for no longer than necessary, anonymisation .....	65
7.3.6	Principle 6 – Information Security .....	66
7.4	International transfers.	68
8	Risks to data subjects rights and freedoms. ....	69
9	Necessity and Proportionality Assessment .....	82
10	Document control.....	87
10.1	Approval - Signoff	88
11	APPENDIX A – Citizen engagement – Privacy Notice questionnaire .....	89
12	APPENDIX B – App Governance .....	90
13	APPENDIX C – Digital and Data Ethics Summary .....	92
14	APPENDIX D – Risk scoring system .....	95
15	Glossary, abbreviations and endnotes .....	99



## 1 The Protect Scotland App

The Scottish Government is introducing a mobile application called 'the Protect-Scotland app' as part of its [Test and Protect' programme](#) '. The app, which will be entirely voluntary for the public to download and use, is intended to act in parallel, and augment the Public Health Scotland's COVID-19 contact tracing service, assisting in breaking chains of transmission, and reducing the spread of the viral infection within the community.

The purpose of this document is to transparently assess the impact of the envisaged processing operations on the protection of personal data, and demonstrate how the rights to privacy and confidentiality of the users are appropriately protected. In light of the scale of the envisaged data processing, types of data processing, and use of new technology; the carrying out of this assessment is considered appropriate.

## 2 Overview

The app is being developed because mobile technology can help and support the current manual contact tracing process, alerting people who have been in close contact with individuals who have tested positive; with speed and accuracy.

With this app, we will no longer have to solely rely on a person who has COVID-19 to know and remember everyone they were in contact with.

This app will quickly and anonymously notify app users who have been exposed to COVID-19 by coming into contact with another app user who has tested positive. The app will tell them to commence isolation and to get tested as well as where to obtain further advice. This is crucial for preventing onward transmission of the infection, helping us stay ahead of the pandemic and save lives.



The app will also allow Scotland to manage more efficiently hot spots detected in specific areas and, overall, minimise the impact on our society and economy by not having to use broad-focused control measures.

The primary purpose of the app is to support the public health response to the COVID-19 crisis in Scotland and accomplishes that through the following functions:

- Remembering when you have been close enough for long enough to other app users during the last of 14 days (interchanging anonymous random keys)
- Registering anonymously positive test results and providing you with immediate advice
- Sending you alerts ('Exposure Notifications') if you have been in close contact with another app user who has tested positive for COVID-19 within the last 14 days. The app will advise you to commence isolation and to get tested. The app also points you to other useful information sources.

The app produces aggregated and anonymous Scotland-wide metrics that will enable the Scottish Government and Public Health Scotland to better understand the spread of the virus and plan accordingly, in particular:

- The total number of app users
- The total number of instances where an app user has registered a positive test result and has consented to upload the encrypted anonymous random codes that will be used to alert other app users that they have been in close contact with over the last 14 days (this is also referred to as 'uploading diagnosis keys')
- The total number of alert notifications triggered (this is also called 'exposure notifications').



As a precaution, in data protection legislation terms, we treat these metrics with the equivalent security rigour as that required for Special Categories of data, as strictly as they were identifiable health data, even though these metrics are anonymous and aggregated.

The collection of these metrics is also essential to prove efficacy and gain CE marking<sup>1</sup> accreditation for the app in line with current regulations set by the Medicines and Healthcare Products Regulatory Agency (MHRA). This app is being rolled out in compliance with these regulations; we must collect these metrics during the next six months to demonstrate efficacy and therefore, gain the corresponding accreditation.

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 be required to improve performance within the scope of existing features as outlined above.

The Scottish Government is considering the future development of versions of the app, to address accessibility, e.g. in terms of languages other than English.

Any future changes to the fundamental features outlined in this privacy notice will follow rigorous information governance processes; the decision will be balanced against public health benefit and cost (balanced against other health priorities) and this privacy notice will be updated accordingly for transparency.

As part of this information governance process, from the early stages of the design of the app, a consultation with relevant Scottish groups of interests and advocacy has taken place, including:

---

<sup>1</sup> **CE marking** is a certification mark that indicates conformity with health, safety, and environmental protection standards for products sold within the European Economic Area.



- The Health and Social Care (Scotland) Public Benefit and Privacy Panel
- The Scottish Privacy Forum
- The Open Rights Group
- The COVID-19 Data and Intelligence Network – Data ethics and public engagement subgroup.

### 3 Roles and Responsibilities

The Scottish Government is the lead organisation for the Protect-Scotland App. It determines the means and purposes of the processing along with Public Health Scotland and NHS National Services Scotland. These organisations are, therefore, the data controllers. Table 1 describes the key organisations involved in the development, management and roll out of the Protect Scotland App, and their specific roles and responsibilities. as data controllers, data processors or third party subcontractors.

A Protect Scotland App Short Life Working Group (SLWG) has been established as a sub-group of the Test & Protect Operational Steering Group. The SLWG has day to day governance responsibility for the development of the app and ensuring national delivery. The SLWG comprises of senior clinical and technical leads under the direction of the Test & Protect Operational Steering Group. Refer to APPENDIX B – App Governance, for further details on membership of the Short Life Working Group and the governance approach.



Table 1 Key organisations and data controllers.

Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<b><u>Scottish Government</u></b> <b>(Scottish Ministers)</b>	Is the organisation responsible for assisting Ministers in discharging their duties with NHS Scotland and the population of Scotland. Scottish Government is the lead <u>data controller</u> for the app and has decided the means and purposes for the processing of data collected and used by the app. The Scottish Government provides strategic direction for the app.	Purpose of the app, technical means to process the data (e.g. the app), technical interchanges of data (e.g. with Test Results, CMS <sup>3</sup> ), how SMS will be sent.	No.  Scottish Government has no access to the data.  Scottish Government and Ministers may receive aggregated statistics on uptake and efficacy of the app, as well as aggregated statistical data for planning the response to COVID at regional (Scotland) level.	Lead data controller as per the duty of Scottish Ministers to protect public health ( <u><a href="#">The Public Health etc. (Scotland) Act 2008 Section 1</a></u> )

<sup>2</sup> Based on the ICO checklists. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/controllers-and-processors/>



Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<a href="#"><u>Public Health Scotland (PHS)</u></a>	<p>Is the organisation responsible for public health matters in Scotland.</p> <p>Scottish Government, through its Directorate for Population Health and the Chief Medical Officer, works closely with Public Health Scotland, to ensure the appropriateness of the app for helping the public keep up to date with the latest advice on the COVID-19 pandemic, but also for planning services and resources, so they are directed to areas of highest risk. Epidemiologists, among other experts, are involved in the assessment of the effectiveness of the app for the broad public health purpose.</p>	<p>Advisory to SG on the potential efficacy of the app for making public health decisions and, about COVID-19 measures.</p> <p>Decides on sharing data with the app (mobile numbers collected in the CMS).</p> <p>They have appointed NSS to manage the National Contact Testing Centre (NCTC) on their behalf.</p>	No.	<p>Controller</p> <ul style="list-style-type: none"> <li>- PHS have a common objective with the Scottish Government regarding the use of the app for public health purposes.</li> <li>- PHS are responsible for the same set of personal data used by the App as Scottish Government.</li> <li>- they have common IG rules to the other data controllers (NHS Scotland IG rules).</li> </ul>



Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<p><b><u>NHS National Services Scotland</u> (NHS NSS)</b></p>	<p>Is the organisation responsible for the National Contact Tracing Centre, on behalf of Public Health Scotland. They operate the Case Management System, which shares data (mobile numbers of people with a positive result) with the app.</p> <p>NHS NSS also manages the contract with NearForm and the contractual relationship with App Users (Terms and Conditions) of the App on behalf of the Scottish Government.</p>	<p>Joint decision (with PHS) on sharing data with the app backend (mobile numbers collected in the CMS and relevant data for self-isolation notification).</p> <p>Triggers the automated process to send the SMS to people who tested positive.</p> <p>NSS receives data from the app to confirm that an SMS has been sent to the user or an error code has been returned.</p>	<p>Yes.</p> <p>NSS is the source of mobiles numbers and relevant dates for self-isolation advice (e.g. date of last test or date of first symptoms).</p> <p>NSS receives "SMS Job reference" data (anonymous) for reconciliation purposes.</p> <p>NSS receives anonymous metrics to provide intelligence services to the Scottish Government, and Public Health Scotland needed for planning the COVID response.</p>	<p>Controller</p> <p>NSS has a common objective (contact tracing) with the Scottish Government and PHS.</p> <p>NSS processes data (mobile numbers and test results) for the same purposes as the other data controllers.</p> <p>Uses common NHS Scotland IG rules, as well as the other data controllers.</p>

Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<p><b><u>NES Digital Service</u></b> (NDS) - (part of NHS Education for Scotland (NES))</p>	<p>NES is a data processor commissioned by the Scottish Government to manage the digital infrastructure required for the app through their Digital Service, in particular, to provide the AWS account for hosting the App backend and to upload the app to the Google Play Store and the Apple App Store.</p> <p>Since NHS Education for Scotland provides various services unrelated to the app, we refer to their engagement as data processor for the app in this privacy notice as NES Digital Service (NDS).</p> <p>NHS Education for Scotland is the legal entity.</p>	<p>NES makes some decisions on how data is processed, but implement these decisions under a contract with the Scottish Government as the commissioner.</p> <p>NES subcontracts Amazon Web Services (AWS).</p> <p>NES owns the AWS account that is being used to host the App backend that provides the centralised data processing.</p> <p>NES also owns the Google Play Store and Apple App Store accounts that will be used to upload the Protect Scotland App to these stores. NES will upload the app; no other organisation will be provided with access to the accounts.</p>	<p>No.</p> <p>NES only has indirect access for the provision of infrastructure services through Amazon Web Services (subcontractor).</p>	<p>Data processor</p> <ul style="list-style-type: none"> <li>- Follows instructions from the Scottish Government</li> <li>- Is told about what data should be processed in the App Backend infrastructure.</li> <li>- Doesn't decide what data to collect, legal basis, purposes, or data sharing.</li> <li>- NES does not benefit from the processing of the data used by the app.</li> </ul>



Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<a href="#"><u>NearForm</u></a>	Is the organisation responsible for developing the app, as well as designing the architecture and delivering essential components (e.g. SMS's code integration).	<p>NearForm develops the code for the app and provides some technical support, and therefore makes some decisions on how data is processed and what data is needed to make the code work but does not decide on the purpose of the app or the functionality that is required.</p> <p>NearForm develops the codes and provides support under contract with the NHS National Services Scotland on behalf of the Scottish Government.</p>	<p>No.</p> <p>Nearform may have indirect access to anonymous data if required for the provision of app technical support services.</p> <p>Nearform will also produce an aggregated SMS failure report; however, no personal identifiable data is accessed to produce this report, only SMS failure notifications.</p>	Data Processor

Organisation	Description	Decisions over the App	Direct processing of personal identifiable data	Data Protection Role <sup>2</sup>
<p><a href="#"><u>Gov.UK Notify</u></a> <b>service (UK Government)</b></p>	<p>The Cabinet Office acts as data processor for Gov.uk Notify. This service is used to send secure SMS notifications.</p> <p>GOV.UK Notify is built for the needs of government services. It has processes in place to protect user data.</p> <p>On Notify, SMS are encrypted.</p> <p>The Notify team has Security Check (SC) level clearance from United Kingdom Security Vetting (UKSV).</p>	<p>Gov.UK notify does not make any decision over the app but interact with the app in order to send SMS messages.</p>	<p>Yes.</p> <p>Gov.UK receives SMS requests from the App backend, which include the mobile number, the Authorisation Code and the date of the test.</p> <p>Gov.UK verifies the mobile number and delivers the encrypted SMS to the App user mobile phone.</p> <p>Gov.Uk also notifies the App backend of SMS messages that have not been delivered due to failure during the verifications process.</p> <p>Data is only held for 72 hours in order to ensure the SMS text messages are sent.</p>	<p>Data Processor</p>



All the organisations identified in Table 1 have provided input to this DPIA and have been involved in the DPIA validation process.

Advice from independent experts of different professions has been sought, including solicitors, IT experts, security experts, epidemiologists, public health experts, data scientist, data and digital ethics experts, Data Protection Officers and Caldicott Guardians.

Information Security Officers and DPOs from Scottish Government and NHS Scotland, have been involved in the Information Security risk assessment and determining whether the residual risk is acceptable, and developing knowledge specific to the app context in Scotland.

## 4 Processing Overview

Use of the App will be entirely voluntary and will be available to download for free from the Apple App Store and the Google Play Store. It will run on iPhones that support iOS 13.5 (or later) and Android phones running Android 6.0 and higher. The functions of the app that fulfil the stated purposes are as follows:

- Contact tracing
- Anonymous aggregated reporting metrics for COVID-19 response planning and research
- 'Leave' function
- Management of App settings

These functions are explained in detail in the following sections.

The app does not collect information on the user's identity or location or track app users. The Scottish Government has also chosen not to include any additional features in the app that capture user data.



Any future changes to the fundamental features outlined in this document will follow rigorous information governance processes; the decision will be balanced against public health benefit and cost (balanced against other health priorities) and this document, as well as the corresponding privacy notices, will be updated accordingly for transparency.

Figures 1 and 2 illustrate how the app works from the a user and technology perspectives.

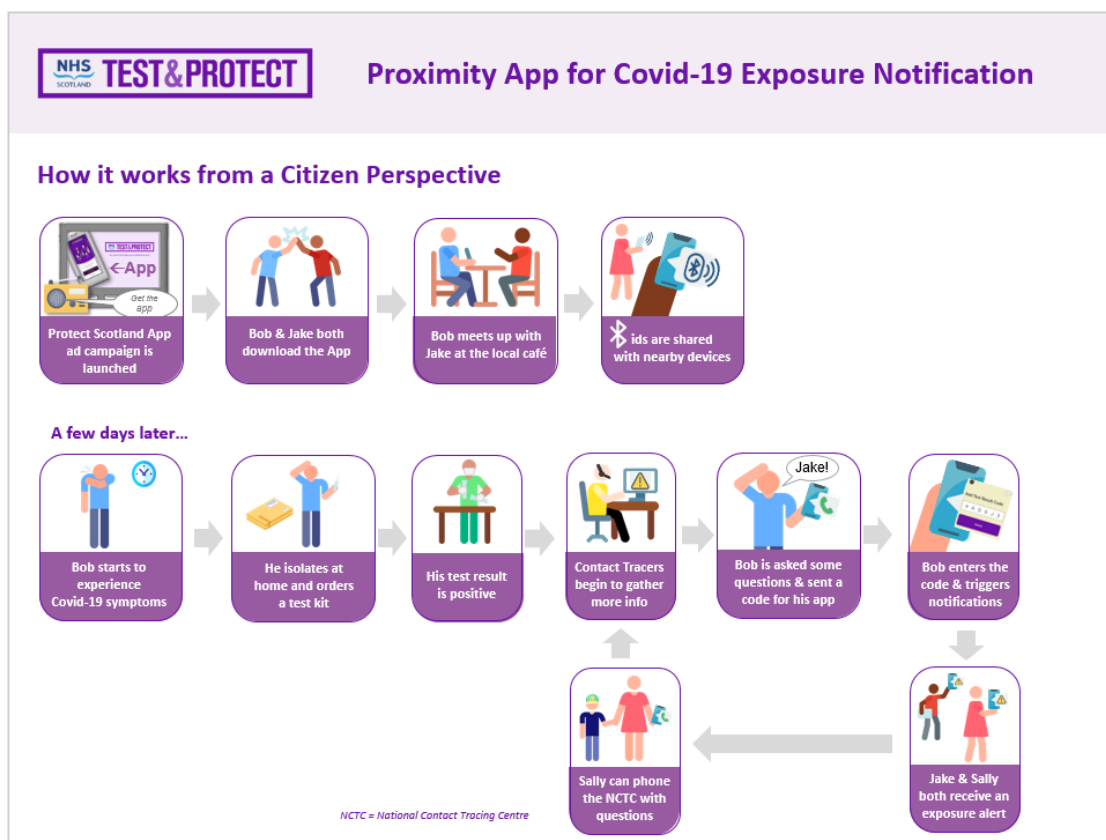


Figure 1 How the app works (Citizen's perspective).



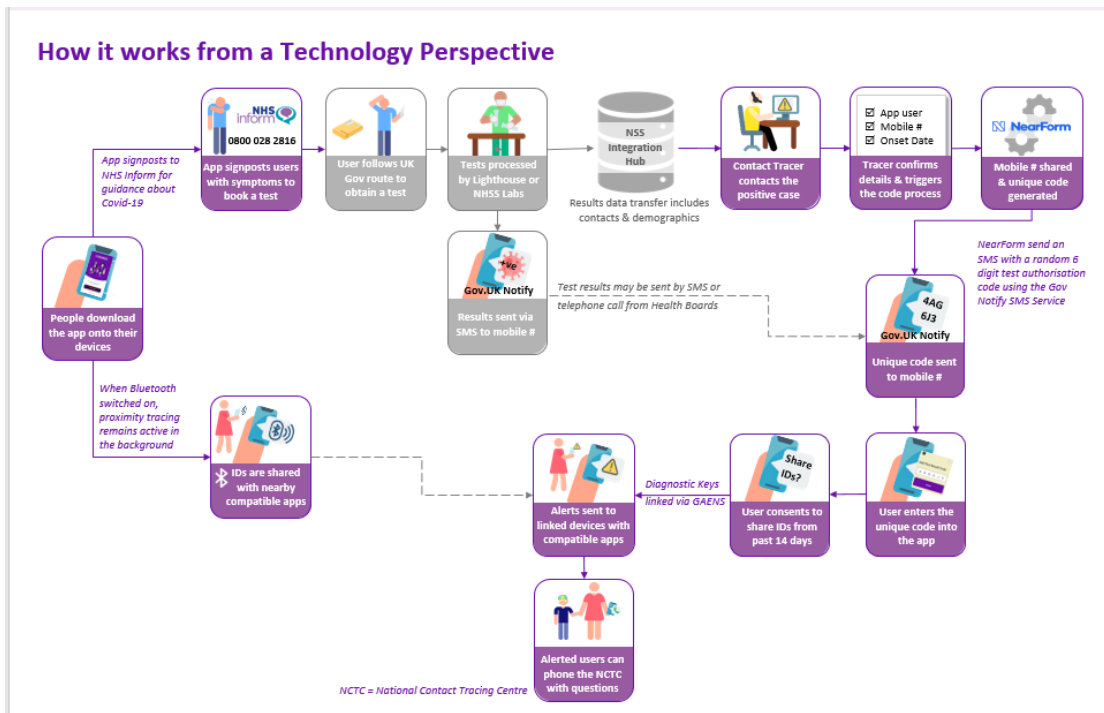
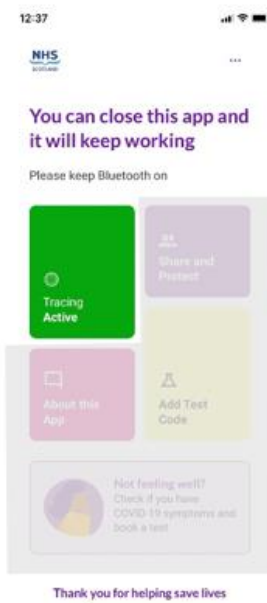


Figure 2 How the app works (Technology perspective). Note: Areas in grey denote processes taking place outside the app.

## 4.1 Contact Tracing



Public Health Scotland has commissioned NHS National Services Scotland to manage the NHS Scotland National Contact Tracing Centre. At the moment, this is a mainly manual process where a person who has been infected with COVID-19 is interviewed over the phone to identify the people they have been in close contact with recently (also called 'high-risk contact').

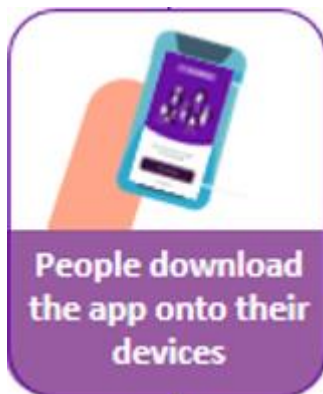
A 'high-risk contact' is defined as having occurred where two people spend more than 15 minutes within 2 meters of each other. These close contacts are then phoned and advised self-isolate. The period given for self-isolation varies and is adjusted according to scientists recommendations; policy decisions on this regard are adapted from time to time as required under the circumstances of the pandemic.



It is estimated that over two-thirds of individuals<sup>4</sup> who test positive have **no symptoms at the time of testing**. The process of asking the ‘high-risk contacts’, of those who test positive, to self-isolate is a proven method of reducing the rate of spread of infection (stopping those with no symptoms spreading the disease onwards).

The Contact Tracing functionality delivered by the app is being designed to augment the current manual contact tracing operation in Scotland, not to replace it; and is proposed to work as follows.

### Exposure Notification’ Services (ENS) service



When a person downloads the app they are asked to enable its contact tracing function. If they choose to do so, the person will be asked to turn on the phone’s ‘Exposure Notification Service’ (ENS).

ENS is a new Bluetooth feature that Apple and Google are introducing to support contact tracing efforts across the globe using iPhones and Android phones in a privacy preserving way<sup>5</sup>. There are further details about ENS in section 4.6 (Exposure Notification Services).

---

<sup>4</sup> ONS survey data.

<sup>5</sup> The description of Exposure Notification Services and how it is used in this document is abbreviated and approximate, removing much of the cryptographic underpinnings in an effort to more clearly impart the key matters relating to data protection. For a full explanation of this service please refer to the Google and Apple documentation - <https://www.google.com/covid19/exposurenotifications/> | <https://www.apple.com/covid19/contacttracing>



## Continuous scanning



Phones with ENS active will continuously scan for other phones nearby with ENS active. When proximity is detected, the phones record this by sending each other random IDs (or in other terms anonymous ‘Identifier Beacons’) without the need for any user action; this includes information on Bluetooth signal strengths to be used later for estimating distance. It does not collect information on the user’s identity or location.

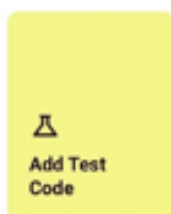
A rolling 14 days’ worth of these IDs and accompanying proximity information, recording a person’s recent encounters, are securely stored on the user’s phone. Still, they won’t have visibility of them, nor can anyone else. This exchange of anonymous ‘Identifier Beacons’ cannot identify people to other app users, nor the



Scottish Government. **These IDs cannot be used to identify individuals.**

ENS, and thus Contact Tracing can be turned off and on, independent of the other app functions, at any time.

## Positive diagnosis and ‘Authorisations Codes’.



If a person tests positive for the virus, the app user will be contacted by the National Contract Tracing Centre as described in their separate privacy notice and DPIA. This is an established process; this app is not changing this manual process; however, the app augments the



existing process by sending an automated SMS<sup>6</sup> containing a random 6 digit alphanumeric ‘authorisation code’, along with the date of the test and a unique “Job Id” identifier to ensure the validity of the message.



The SMS will not be sent under the following circumstances:

- The National Contact Tracing Centre doesn’t have a valid mobile phone number available for the recipient (the person who tested positive),
- The person is under 16 years old

The source of this contact details is information volunteered by a person when booking a test.



The National Contact Tracing Centre, using their Contact Management System (CMS) will pass this information to the app backend in order to generate the ‘Authorisation Code’ and send the SMS.

This information is not stored anywhere. The App backend (hosted within the AWS) deletes the SMS message containing the “Authorisation Code” once it has been generated and sent to Gov.UK Notify.



The SMS text message is delivered using the Gov.UK Notify service <https://www.notifications.service.gov.uk/>, a secure

SMS service specific for the government security requirements within the UK.

---

<sup>6</sup> SMS (Short Message Service), is a text messaging service used by most mobile devices. It uses standardized communication protocols to enable mobile devices, apps and other information systems to exchange short text messages.



Gov.UK Notify retains the SMS for up to 72 hours as, sometimes, sending the SMS may require several attempts, then is deleted.

The 'authorisation code' contained in the SMS will remain valid for 24 hours.

In order to ensure there is no risk of re-identification of mobile numbers at any later stage, the app backend has been physically and logically split into two different and separate areas, one provides "authorisation codes" functionality, and the other one offers the rest of the app functionality.

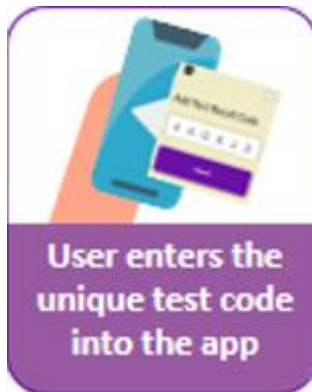
The app backend is hosted in the AWS cloud infrastructure (based in London) and is managed by the NES Digital Service (NDS) on behalf of Scottish Government.

The National Contact Tracing Centre does not know who is using the app; therefore, the Case Management System automatically generates and sends an SMS message to all positive test cases for people who are 16 years old or over and have a registered mobile phone number on their records.

All people with a positive test will also receive a phone call from the NHS National Contact Tracing Centre as part of Scotland's 'Test and Protect' programme run jointly by the Scottish Government and the NHS Scotland.

On the call, they will be asked if they are using the app and if so if they have received an authorisation code via SMS. If the app user informs the contact tracer that they have not yet received an SMS "authorisation code" or that their authorisation code has expired (they are valid for 24 hours), the contract tracer will be able to check the mobile phone number in their CMS record and to generate another immediate request to send them another authorisation code.

## Inputting the Authorisation Code and uploading Diagnosis Keys.



Once the app user has their authorisation code, they will be presented with an option to input it in the app. Inputting the Authorisation Code is entirely voluntary. When the code is entered into the app, this authorises an upload of their anonymised IDs (or 'identifier beacons') generated by the phone over the last 14 days. These IDs are then called 'diagnosis keys'.

Diagnosis keys are stored in the "AWS Registry", a physically and logically separate section of the app backend architecture hosted in a secure environment in the AWS cloud infrastructure.

In order to send the Diagnosis Keys through the network, they are attached to the IP address of the sender (the app user) and the recipient (the app backend) as well as some security keys. At this point, the Diagnosis Keys are considered personal health data and is sent encrypted.

On entry to the backend architecture, the IP address is stripped off the 'diagnosis keys' (and not retained anywhere) rendering the 'diagnosis keys' completely anonymised.

## Exposure notification alerts.



The backend architecture then makes these anonymised 'diagnosis keys' visible to instances of the app on other users phones, covering only the infectious period of 14 days (this is known as 'publication').

This enables other app users who have been in high-risk contact with an app user (who has tested positive) to be notified.



The app checks the newly published 'diagnosis keys' every two hours. The matching process takes place in the App User phone. At this point, no App User data is sent to the App Backend for matching, but rather pulls published 'diagnosis keys' and performs the checks within the App User phone. If there is a match between stored close contact IDs, ('identifier beacons'), from the previous 14 days, and newly published 'diagnosis keys', an exposure notification is triggered. The notification advises the user to self-isolate and to get a test if they develop symptoms. The app also provides a link to further information, including a number to call if they have issues relating to the notification. **Identification of app users is not possible at any point in the 'exposure notification' process.**

The app has the advantage of notifying 'high-risk contacts' who are app users, who may be unknown to the person testing positive. The app improves the possibility of breaking chains of transmission of the viral infection, notifying unknown 'high-risk contacts' promptly (within a couple of hours of a test result being known). The manual process takes up to 24 hours at present; and in a period of peak demand, this may extend further.

Exposure notifications remain visible on the app for 14 days from the date of last exposure. Users can clear exposure notifications from their app at any time via settings. If a user receives multiple exposure notifications relating to different exposure events, they only receive a new alert if the exposure notification relates to a more recent exposure event.

For the app to work as described, app users have to allow 'COVID-19 Exposure Notification Services' on their phones. An option is provided to the app user to enable this service as part of the app set up.

People can also choose to allow their phone to display notifications so that they also receive a phone alert when they have been exposed to someone who has tested positive for COVID-19. An option is provided to the app user to enable these alerts as part of the app set up. App users can turn on and off this functionality in the settings page of the app at any point in time.

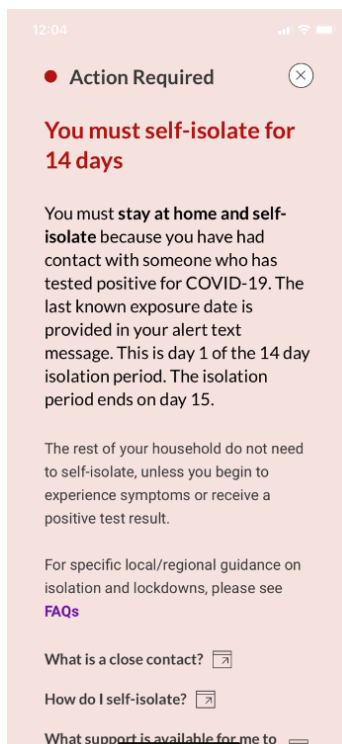




It is important to note that none of the helplines mentioned in this Privacy Notice will reveal the identity of any person using the app to other app users, and never reveals who has been diagnosed positive.

When someone receives an exposure notification via the app, they are advised to self-isolate and book a test if they become symptomatic. The phone number of the user receiving a notification, or the number of the person testing positive, are not visible via the app, and will not be shared. Furthermore, the Scottish Government or the NHS Scotland will not be aware of an exposure notification in any way. If a person self-isolating after an 'exposure notification' becomes symptomatic and books a test, should the test be positive, they will be followed up in the manual tracing process. If they are also an app user, and have registered a contact mobile number, they will receive a 6 digit 'authorisation code' for input, independently of the manual contact process.

### Automated decision-making.



The generation of exposure notifications advising to self-isolate and get tested 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' mobile phones have been in close proximity, for a sufficient period of time to mean that it is possible that the coronavirus has been passed on.

This processing is explained in the terms and conditions of the app. Users must accept the terms and conditions if they want to download and use the app. There is a contact number at the end of this privacy notice if you need to discuss this with someone.



App users have the right to contest this automated advice to self-isolate and get tested if they feel this may significantly affect them. In this case, they can call NHS 24 to speak to a person or, if they already have a designated contact tracer, they may wish to discuss their situation with them.

## 4.2 Reporting metrics.

The app produces aggregated and anonymous Scotland-wide metrics that will enable the Scottish Government and Public Health Scotland to better understand the spread of the virus and plan accordingly, in particular:

- The total number of app users
- The total number of instances where an app user has registered a positive test result and has consented to upload the encrypted anonymous random codes that will be used to alert other app users that they have been in close contact with over the last 14 days (this is also referred to as ‘uploading diagnosis keys’)
- The total number of alert notifications triggered (this is also called ‘exposure notifications’).

The collection of these metrics is also essential to prove efficacy and gain CE marking accreditation for the app in line with current regulations set by the Medicines and Healthcare Products Regulatory Agency (MHRA). This app is being rolled out in compliance with these regulations; we must collect these metrics during the next six months to demonstrate efficacy and therefore, gain the corresponding accreditation.



### 4.3 Leave function

The app provides a leave function that can be used at any time. Selecting this deletes all app data from the phone. The user will be notified that they can also delete ENS data via the phone device settings as the app does not have direct control or access to ENS data. If Leave is selected, non-identifying security token data that is used to associate valid (device integrity checked) apps with the app backend are removed from the app backend. If the app is deleted from the phone, it has the same effect as 'Leave', however, the security tokens are not removed as the app backend has no way of knowing – they will be deleted after 60 days of not being used.

#### Leave

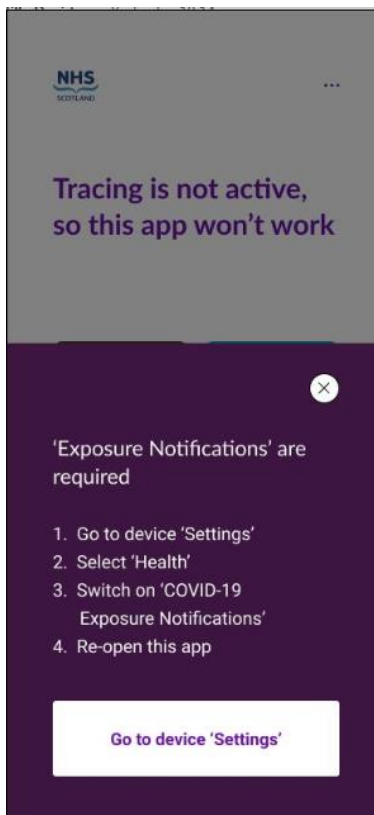
Thank you for helping to fight COVID-19. We're sorry to see you go. When you tap 'I want to leave' we will remove all data stored by the app from your device.

Random IDs created or collected by Exposure Notification Services cannot be removed by this app. If you want to remove these, do this through your device 'Settings'.

I want to leave



## 4.4 Management of App settings.



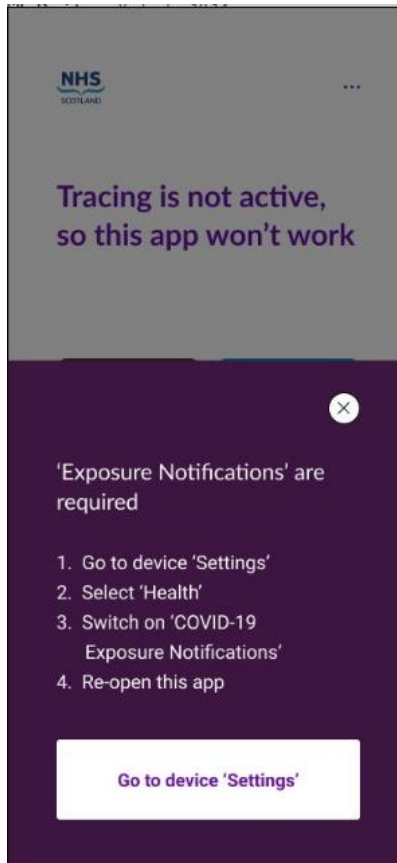
- The phone operating system allows control of the Bluetooth and Notifications settings. If these functions are disabled, the app alerts the user to this.
- If the Contact Tracing function is off, the user is alerted and directed to the ENS phone settings where it can be turned on or off.
- Bluetooth is necessary for the operation of the Exposure Notification Service.
- Notifications can be switched on and off from the phone operating system notifications settings.
- Exposure notifications can be cleared from the app.
- The app settings menu also offers a link to the 'terms and conditions', and a the 'privacy notice'.

## 4.5 Download and Installation

To install the app, a user downloads the app from either the Google or Apple app stores. Each store will keep a record of the user's download of the app using their unique identifier, AppleID or GoogleID, within the store. Apple and Google are Data Controllers in respect of their respective app stores and gather certain statistics about app usage, such as number of downloads and number of deletions. More information is publicly available in regards to how data is processed by the app stores.



## 4.6 Exposure Notification Services



It is worth going into further detail on the workings of the 'exposure notification' service (ENS) at this stage to support the rest of this section.

Each phone that has ENS switched on generates a random daily key, which is stored on the phone, and called a 'Temporary Exposure Key' (TEK).

These keys are used to further generate random IDs approximately every 15 minutes called 'Rolling Proximity Identifiers' (RPI) (referred to above as 'identifier beacons', Random IDs or ID 'keys'), which are used to send to other ENS enabled phones when nearby. RPIs are accompanied by Associated Encrypted Metadata (AEM) data, which includes protocol versioning and Bluetooth transmission power.

With the App User authorisation, Random IDs are uploaded into the App Backend (the AWS Registry) on positive diagnosis; at this point they are called 'diagnosis keys'. Keys uploaded to the AWS Registry are publically available, downloaded by all apps, and used to regenerate the RPIs – which are in turn used to check for a match, on the phone, in order to generate an exposure notification. RPI and AEM data are processed on phones only (not available directly to contact tracing apps). These keys are stored for 14 days; are not capable of being used to identify a person; and are not considered personal data (the IP address having being deleted at the networking layer as described earlier).

There is more information about ENS here:

<https://www.google.com/covid19/exposurenotifications/>



### 4.7 Systems involved

Personal data will be collected, processed and stored in the following locations and IT systems:

- The app on users' mobile phones
- The app backend hosted within AWS and managed by NES Digital Services.
- Gov.UK Notify servers

Figure 3 illustrates the systems involved. Data is encrypted in all these locations.

This section describes the IT systems and other App related services that will be used for the appropriate of the Protect Scotland App. Further technical documentation, including the source code of the app is available here:

<https://github.com/NES-Digital-Service/protect-scotland>

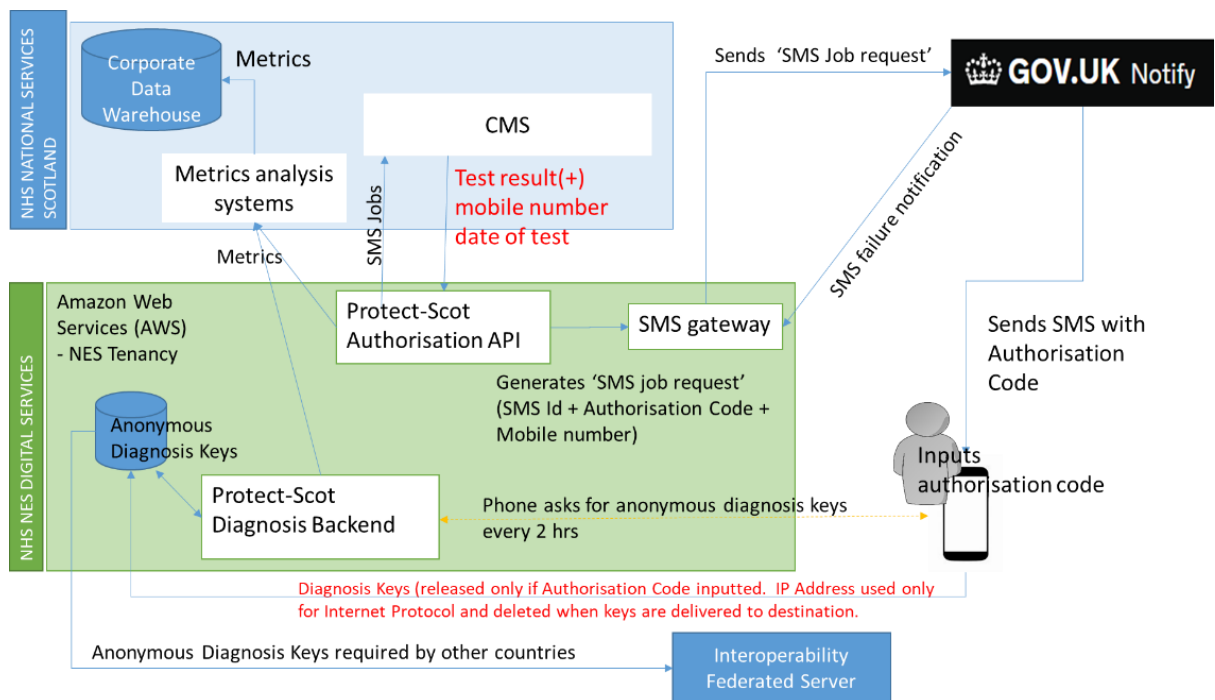


Figure 3 Systems where data is processed. Identifiable (in red) and non-identifiable data (black).



#### 4.7.1 The Protect-Scot App (Android and IOS)

The app is available to download from either the Google or Apple app stores. Users. Each store will keep a record of the user's download of the app using their unique identifier, AppleID or GoogleID, within the store. Apple and Google are Data Controllers in respect of their respective app stores and gather specific statistics about app usage, such as the number of downloads and number of deletions. More information is publicly available in regards to how the app stores process data:

- <https://www.apple.com/uk/legal/privacy/en-ww/>
- <https://policies.google.com/privacy>

The App front end has been developed by NearForm, the company which built the App for Ireland's health authority and Northern Ireland Department of Health.

The code has been donated as an open-source project. Open source, denotes software for which the original source code is made freely available and therefore can be studied or re-used by anyone. Open source software has many benefits, but particularly on superior assurance and security, not only because more people can see and identify potential security problems, but also because security issues ('bugs') tend to be fixed faster.

The front end of the Scotland Protect App, which operates on users phones, does not collect any personal identifiable data. Still, for a few seconds at a time, it generates and sends (upon authorisation from the user) Diagnosis keys, which are considered personal identifiable health data. This is explained in detail in the "Personal Data" section under Diagnosis Keys and IP Addresses.

#### 4.7.2 The App backend.

The app backend is also part of the NearForm code. It includes two physically and logically separate components:



- The Authorisation API, which generates the authorisation codes and SMS for people who tested positive.
- The Diagnosis Keys backend, which uploads, stores and makes visible the anonymous diagnosis keys for those who tested positive and decided to upload their keys for other app users to receive exposure notifications.

These components are hosted by Amazon Web Services (AWS) (London Region) in a dedicated and restricted secure environment of their cloud services, the so-called 'tenancy' or 'account' of NES Digital Services to manage the infrastructure used for the app.

#### 4.7.3 Other systems.

The App backend interacts with the following external systems.

- **Gov.UK Notify** - The SMS text message with the Authorisation Code is delivered using the [Gov.UK Notify service](#)<sup>7</sup>, a secure SMS service specific for the government security requirements within the UK. GOV.UK Notify is built for the needs of government services. It has processes in place to protect user data, keep systems secure and manage risks around information. On Notify, data is encrypted when it passes through the service and when it's stored on the service. Any app user data uploaded is only held for 72 hours. Scottish Government is the data controller for any app user data uploaded on Notify and the Cabinet Office is the data processor responsible for Gov.UK Notify. This service is compliant with the National Cyber Security Centre (NCSC) Cloud Security Principles. There is more information about the security of Notify here:

<https://www.notifications.service.gov.uk/features/security>

---

<sup>7</sup> <https://www.notifications.service.gov.uk/>

- **NHS SCOTLAND (NSS) Corporate Data Warehouse** - the anonymous metrics stored in the App backend will be accessed by the Corporate Data Warehouse for reporting (e.g. analytical dashboards) purposes. This data is anonymous and aggregated at regional (Scotland) level.

#### 4.7.4 Federated interoperability

Federated Interoperability is necessary to allow people to travel across countries and to ensure exposure notifications still will operate across countries, in line with EU recommendations.

Cross border interoperability is something that the European Commission and separately Google and Apple are working on. Scotland is working in cooperation with counterparts, including the Republic of Ireland and the wider UK Government, to deliver interoperability to EU requirements.

At present, the app is not sharing any data with any “federated interoperability” servers; the Scottish Government is currently looking at options. This DPIA will be updated once it is clear what server will be used.

The ‘diagnosis keys’ processed by a Federated Interoperability server are anonymous. The IP address is stripped from the ‘diagnosis keys’ on entry to the app backend before the non-identifiable keys are passed on securely to the federated server. The infrastructure will be set out in this section as soon as the option that Scotland is going to take for this purpose is clear.

The associated Memorandum of Understanding (MOU) for governing the functioning of the ‘federated server’ and the sharing of anonymised ‘diagnosis keys’ will be made publicly available at <https://protect.scot/> (transparency section).





## 4.8 Disclosures of personal data.

- Personal data is shared with the third parties set out in Table 2 for the purposes/activities mentioned in section 5.2.1 (5.2.1 Purposes for which personal data is used.).

*Table 2 Disclosures of personal data.*

Personal data	Party with whom personal information is shared
Mobile phone number	Data processors: <ul style="list-style-type: none"> <li>• NHS Education Scotland (NHS NES) who manage the digital infrastructure required for the app under a contract with Scottish Government</li> <li>• UK Government’s Gov.uk Notify text service who send the authorisation codes and advise of successful delivery or non-delivery under a contract with NHS NES</li> <li>• Amazon Web Services who host the app under a contract with NHS NES</li> </ul>
Estimated date of infection	Same as above
Authorisation code	Same as above
IP address	Data processors: <ul style="list-style-type: none"> <li>• NHS NES</li> </ul> Amazon Web Services
Exposure notification	Data processors: <ul style="list-style-type: none"> <li>• NHS NES</li> </ul> Amazon Web Services
Your confirmation of app use	Data processors: <ul style="list-style-type: none"> <li>• NHS NES</li> </ul> Amazon Web Services

The app can only be downloaded from the Apple app Store and the Google Play Store. In this regard they are independent controllers as owners of the app stores. Their processing activity is separate to the processing of personal information on the app. Furthermore, although Apple and Google have developed the technology on which the app is based, neither company obtain any personal information from the app or the exposure notifications.



#### 4.8.1 Other recipients (anonymous data)

The Scottish Government may make freely available high-level statistical data; this is data at regional (Scotland) level produced using metrics that are explained in section 4.2 (Reporting metrics.). The purpose is to ensure members of the public have visibility of the level of uptake, and the potential of the app to reduce the rate of spread of infections of COVID-19.

## 5 Scope of Processing

This section of the document describes the data that will be processed, how much data is being collected and used, how often it will be processed, how long it will be retained for, and who the data relates to.

### 5.1 Data Subjects

#### Scotland's users

The proposed data processing relates to individuals over 16 in Scotland (residents or travellers - including people who may travel cross-border for work purposes), that choose to download and install the app that have a smartphone capable of meeting the ENS requirements set out previously. The app will be published in the UK app stores only, making clear that it is intended for download by individuals residing in Scotland to download and install it.



Figure 4 Typical categories of app users.

## International users

At present, international visitors can download and use the app when visiting Scotland.

Federated Interoperability will be available at the earliest possible juncture (refer to section 4.7.4 Federated interoperability)

## 5.2 Personal data

A rigorous data minimisation approach has been adopted in relation to the processing of personal data, and only personal data that is strictly necessary for the operation of the app will be processed. Table 3 describes the personal processed by the app.



Table 3 Personal identifiable data processed by the app.

Personal information	Additional details	Where is this information received from?	Retention
<b>Mobile phone number</b>	If your Covid-19 test result is positive, your mobile phone number will be used to provide an authorisation code for you to enter into the app. The app itself does not use your mobile phone number.	This is taken from the Case Management System (CMS) used by the National Contact Tracing Centre. (e.g. from the information you provided when registering for the Covid-19 test).	Not stored.  Refer to retention of SMS data.
<b>Estimated date of infection (*)</b>	If your Covid-19 test is positive, a contact tracer will estimate the date of infection. This is likely to be either the test date or the date of your first symptoms. The estimate can be based on the information you have provided.	This is taken from the CMS used by the National Contact Tracing Centre and is estimated by a contact tracer.	Not stored.  Refer to retention of SMS data.
<b>Authorisation code (*)</b>	If you have received a positive Covid-19 test result, you can enter this random authorisation code into the app to allow the random IDs that were collected during the relevant infectious time period to be sent to the app server and exposure notifications to be provided to other app users. Your authorisation code is sent to you by text message.	This is requested by the National Contact Tracing Centre only if you told them that you are an app user and that you want to receive an authorisation code.  It is provided to you by text message, and is generated by the app and sent to you using the Gov.Uk text service.	Not stored.  Refer to retention of SMS data.
<b>IP address</b>	Internet Protocol (IP) address is a numerical label assigned to your device by the mobile phone or the Wi-Fi service provider. This allows the app to communicate with the internet.	This is assigned to your device by your mobile phone or your router. This is automatically determined by your	Not stored.  Deleted by the network as soon as the data reaches destination



Personal information	Additional details	Where is this information received from?	Retention
		internet service provider.	(typically within seconds).
<b>Diagnosis keys (*)</b>	The app collects anonymous random IDs using Bluetooth technology when app users come into close contact with each other. If an app user receives a positive Covid-19 test result and inputs an authorisation code into the app, the random IDs that were collected during the relevant infectious time period are sent to the app server. These are known as diagnosis keys and are combined with the user's IP address to send the data to the app server, after which the IP address is stripped off so the diagnosis keys are anonymous.	These are generated by the app.	Stored in anonymous format for 14 days in the App Backend (AWS Registry).
<b>Exposure notification (*)</b>	This is a notification provided by the app to an app user who has been in contact with an unnamed person who has tested positive for Covid-19, where the contact was recent enough, and for a sufficient time at a close enough distance, to mean that the app user receiving the notification may have been at risk of contracting the virus.	This is generated by the app.	
<b>Your confirmation of app use</b>	This is your confirmation when you click "yes" to the question "Do you agree to continue and start using this app?" during the initial setup of the app on your device. This is combined with your IP	This is generated by the app after you click "yes".	



Personal information	Additional details	Where is this information received from?	Retention
	address to send the data to the app server, after which the IP address is stripped off so the confirmation of app use is anonymous.		

(\*) Personal information relating to health, either because directly denotes a health aspect of the individual (e.g. estimated data of infection) or by inference (e.g. Authorisation Code, since this is only issued to App Users who have tested positive form Covid-19). Personal health information is considered special category data in terms of data protection legislation.

## Metric Data

We collect and use statistical and aggregated data regarding the total number of app users, the total number of authorisation codes entered by app users and the total number of exposure notifications provided to app users. This is called metric data.

In order to count the total numbers of app users, authorisation codes and exposure notifications, an app user’s device sends a “count” to the app server:

- when you click “yes” to the question “Do you agree to continue and start using this app?”;
- every time diagnosis keys are sent from your device to the app server after you have entered an authorisation code; and
- every time your device gives you an exposure notification.

The app uses your IP address in order to send these “counts” to the App server. At this point this is considered your personal information, because it contains your IP address. Once the “count” reaches the app server (typically in no more than a few seconds), the IP address is deleted, and this “count” becomes anonymous and can no longer be associated with you or any other app user.

Metric data is collected on a Scotland-wide basis and is not considered personal information in law as this data will not directly or indirectly reveal your identity. We may hold this information indefinitely and collect this information to:



- allow us and members of the public to have visibility of the level of uptake and the potential of the app to reduce the rate of spread of infections of COVID-19; and
- to gather information required to obtain formal regulatory approval (from the Medicines and Healthcare Products Regulatory Agency) and accreditation for the app.

### 5.2.1 Purposes for which personal data is used.

Table 4 Purposes / Activity for which data is used.

Personal information	Purpose / activity
<b>Mobile phone number</b>	To send your authorisation code to you by text. Your authorisation code is needed for exposure notifications to be provided to other app users if you receive a positive Covid-19 test result.
<b>Estimated date of infection</b>	To identify the relevant time period during which other app users could have been infected if they were near an app user who has received a positive Covid-19 test result.  The infectious time period is used to identify the relevant random IDs from the app user's device who has tested positive, to allow exposure notifications to be provided to other app users who have been in close contact with the infected app user during the infectious time period and therefore could be at risk of having contracted Covid-19.
<b>Authorisation code</b>	To allow exposure notifications to be provided to other app users, if you receive a positive Covid-19 test result. This is also used to collect metric data.
<b>IP address</b>	To send information from your phone to the app server to allow exposure notifications to be provided to other app users and to collect metric data.
<b>Diagnosis keys</b>	To provide exposure notifications to app users and to collect metric data.
<b>Exposure notification</b>	To inform you that you may have been at risk of contracting the virus and to collect metric data.
<b>Your confirmation of app use</b>	To collect metric data.



### 5.2.2 Data minimisation and anonymisation.

The Protect Scotland App has been designed in a manner to minimise the amount of personal data processed in order to fulfil its defined purposes.

The following are design approaches that highlight putting the principle of data minimisation into effect.

- People are not asked to input any personal data in the app.
- Any data that can be associated to an individual is deleted and anonymised at first opportunity (refer to Figure 1 and Figure 6)
- Mobile numbers are only transferred to the App backend for people who tested positive and want to receive an 'Authorisation Code'.
- The use of a "decentralised" model for the contact tracing function allows phones to process data on a phone to generate close contact warnings locally without having to upload personal identifiable data to a centralised server.
- IP address data that is included in all internet traffic between the app and app backend is not logged and terminates at the API Gateway stage (network load balancer) and is never sent onwards to the application layer. This prevents inadvertent or otherwise recombination of IP address data with any payload data sent by the app to the app backend.
- The retention period for all personal data is set out in Section 5.2.3 of this document and has been carefully examined to be only as long as is necessary for the fulfilling of its purpose.
- Cross pollination of personal data between the primary functions of the app is not performed, and each of the functions can be used without the use of the others.



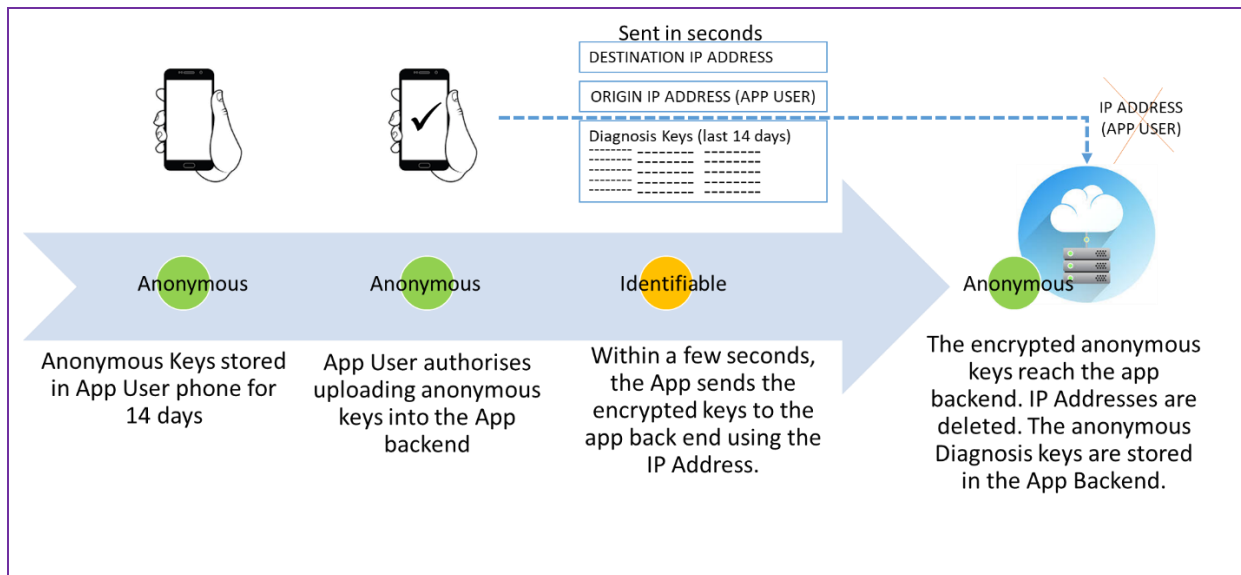


Figure 5 Timeline for anonymisation and retention of diagnosis keys.

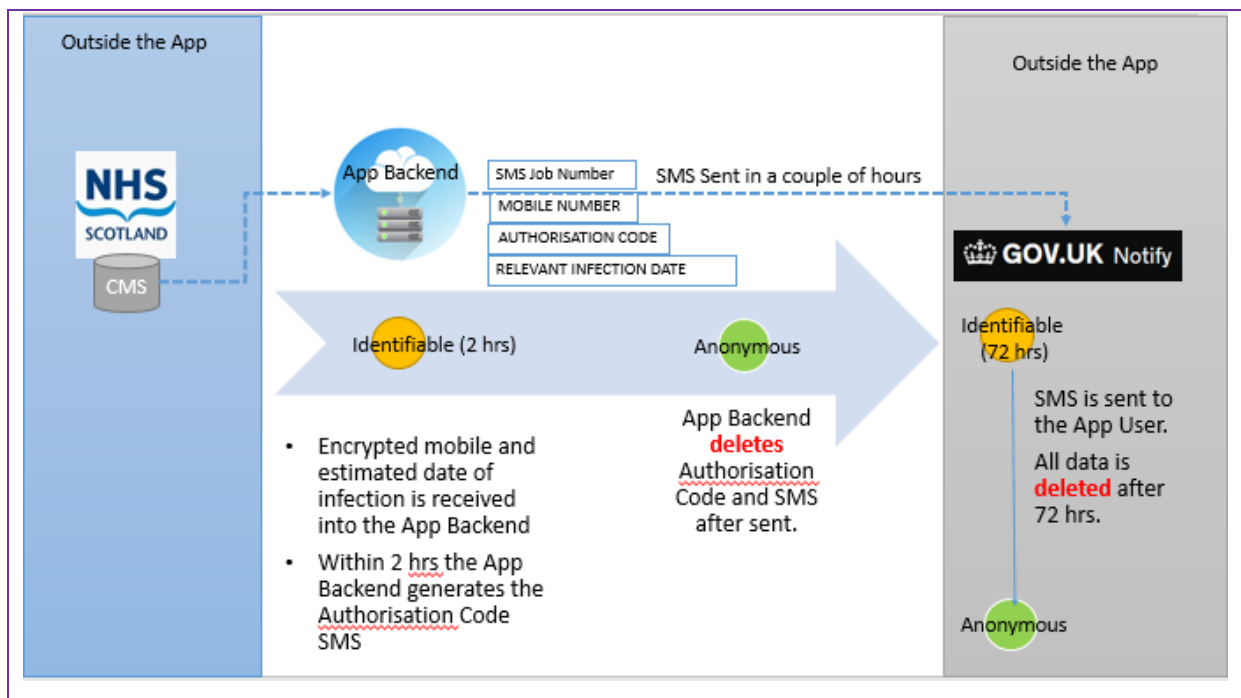


Figure 6 Timeline for anonymisation and retention of SMS Data



### 5.2.3 Data retention

**The app does not store personal data, except for SMS text messages, which are held encrypted by Gov.UK Notify for 72 hrs and then deleted.**

The app does not store personal identifiable data beyond the minimum necessary for the processing.

Table 3 illustrates the retention period for the specific personal data items.

An overarching policy of data retention concerning the app is that no data captured will be processed beyond the period of the pandemic in line with recent European Data Protection Board's guidelines on the introduction of such apps.

The Digital Health and Care Directorate (Scottish Government) is responsible for ensuring that an orderly wind-down of the app and the removal of all data captured is implemented within 90 days of the end of the COVID-19 crisis.

The end of the COVID-19 crisis and the wind-down of the app will be determined by Scottish Ministers taking advice from the Chief Medical Officer in Scotland. The wind-down will include measures such as of the issuance of clear guidelines for app deletion, removal of the app from app stores, the secure destruction of all captured data and diagnosis keys from backend servers, and the shutting down of all app backend services.

Users can delete the app and all data associated with it, from their mobile phones at any time but using the Leave function.

#### **IP Addresses**

Your IP addresses are not retained. They are deleted immediately after use. They are only used to transfer data in the network. Each time the app sends data through



the network uses your IP Address. This is deleted as soon the data reaches its network destination, which typically occurs within seconds.

### **Random IDs (Identifier beacons) on your device**

This is anonymous information. Identifier beacons are retained for 14 days on the mobile phone.

### **Diagnosis keys stored in the secure AWS Registry**

This is anonymous information retained for 14 days to perform an exposure match check and is deleted after that.

### **SMS including mobile number, authorisation code and relevant data of infection.**

All SMS texts and phones numbers processed on the App backend are deleted once an SMS is successfully transmitted.

The Gov.UK Notify service only holds user data for 72 hours. This is necessary in order to ensure the SMS is delivered. Any errors sending the SMS not resolved within 72 hours are reported back to the App Backend for reconciliation purposes and the SMS is deleted from the Notify servers.

### **Metrics**

Regional (Scotland level) statistical summaries of the metric data; these summaries will be retained indefinitely. These summaries do not contain any personal identifiable information, nor individual-level data of any kind; it is aggregated at Scotland level, therefore, unable to be subject in any manner to re-identification. This information will be retained for research and future pandemic response planning and for obtaining formal MHRA Regulatory approval and CE marking accreditation.



## 6 Context of Processing

This section of the document sets out various contextual aspects of the processing with and impact on the privacy by design and by default approach taken. It also sets the context in regards to privacy concerns that people may have with the app.

### 6.1 Design Principles

The core principles guiding the app from design to operation include:

- The app is entirely voluntary to use;
- The app will not ask people to enter personal identifiable data
- The app will give control to App Users about what data or functionality they want to use:
  - The 'App settings' give user the ability to delete the app and any app-related data stored on the phone.
  - Users can decide if they want to allow 'COVID-19 Exposure Notification Services' on their phone.
  - Users can also choose to receive notifications so that they can receive a phone alert when they have been exposed to someone who has tested positive for COVID-19. They can turn on and off this functionality in the 'Notifications' settings of their mobile phone at any point in time.
- The app is used to augment the existing manual contact tracing process;
- The app is used for the purposes set out in the DPIA, and only in the context of the COVID-19 crisis;
- The app is to be decommissioned once the COVID-19 crisis is over;



- The app processes data as set out in this DPIA, the [Terms and Conditions of the App](#)<sup>8</sup> and [Privacy Notice](#)<sup>9</sup>)
- the DPIA and Privacy Notice are accessible to the public and kept up to date
- The app does not use location services to track the location of users or for any other purpose;
- The app does not, and will never, reveal the identity of a person infected with COVID-19;
- The app must be able to function while the screen is locked.

The trust of the public in the proposed processing of data and appropriate privacy measures are of paramount importance to engender the adoption of the app. The Scottish Government is committed to transparency in the development and operation of the app. To that end, the source code and this DPIA document and related documents (e.g. EQIA) will be published to the public online as soon as they are ready.<sup>10</sup> These will be kept up to date to reflect the live operation of the system and the data being processed. Furthermore, robust processes will be put in place to perform security testing and respond to security issues during the development and the operation of the app.

## 6.2 Privacy Model

As mentioned previously, the Contact Tracing function uses a new Android and iPhone service called 'Exposure Notification Service's (ENS). Only nationally recognised health authorities will be able to produce an app that is authorised to use ENS. Apps that do use ENS have limited levels of access to ENS data. Examples of this include – apps are not allowed direct access to the random IDs being exchanged with nearby phones (RPIs) (referred to in this document as 'identifier beacons' and

---

<sup>8</sup> <https://protect.scot/terms-and-conditions>

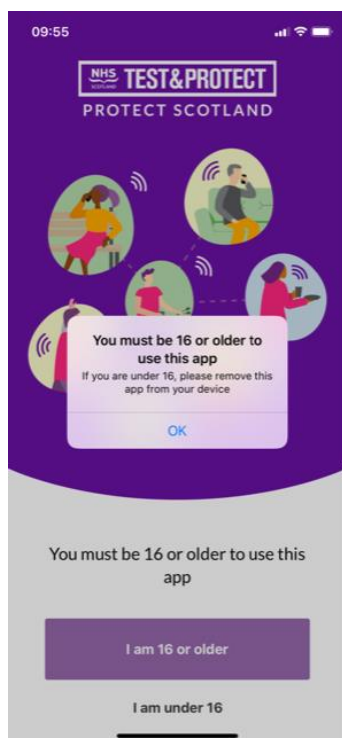
<sup>9</sup> <https://protect.scot/privacy-policy-app>

<sup>10</sup> <https://github.com/NES-Digital-Service/protect-scotland>

ID 'keys'); they are restricted in checking for exposure matches a maximum of 15 times per day; they cannot get access to diagnosis keys without the user's explicit permission. In general, apps are restricted in how they can use ENS to preserve the privacy design of the service. ENS follows what is informally called a 'decentralised' model for mobile app contact tracing, which allows people to get exposure notifications without sharing personal data with a health authority or anyone else. The Scottish Government is committed to this design principle and will independently test the robustness and security of the ENS service. The Protect Scotland App Short Life Work Group (see APPENDIX B – App Governance) will help provide an oversight function; source code data<sup>11</sup> has been made available to the Information Commissioner's Office for scrutiny as part of the process of transparency.

### 6.3 Children

At present, the app is available for people 16 years old or over.



Safeguarding protections would be necessary for individuals under the age of 16 years using the app, necessitating parental consent. This would be problematic as there is no definitive age for children's consent within the UK; and due to anonymity built into the app (by design to be GDPR compliant), gaining parental consent would not be possible. Due to the need for anonymity, there won't be any facility for direct contact with users or a mechanism to monitor this. The Scottish Government would have no way of checking a child's capacity to consent. For that reason, prospective app users will be asked to confirm that they are 16 years or older at the time of downloading the app. Enforcing this is also problematic.


---

<sup>11</sup> <https://github.com/NES-Digital-Service/protect-scotland>



Google Play and Apple stores can potentially restrict downloads from certain age; however, this is not possible to implement since the Protect Scotland App is targeting at present a different limit (16 or older) – therefore these settings cannot be applied.

The Protect Scotland App is currently rated PEGI 3 (content suitable for all age groups) according to the Google apps and games content rating<sup>12</sup>.

Rating	Description
	<p><b>PEGI 3</b></p> <p>The content of apps with this rating is considered suitable for all age groups. Some violence in a comical context (typically cartoon-like – Bugs Bunny or Tom &amp; Jerry – forms of violence) is acceptable. A child should not be able to associate the character on the screen with real-life characters; they should be distinctly fantasy. The app should not contain any sounds or pictures that are likely to scare young children. No bad language should be heard.</p>

Due to the overriding nature of the need to deliver a proximity app solution that meets ICO guidance for anonymity, there is no identified mechanism for further age verification possible. It is seen as a significant challenge to reliably seek parental consent to support younger users of the app at this stage. It is not clear at this time how this can be achieved in a practical way that can scale.

Furthermore, it is not clear the appropriateness of alerting young people with exposure notifications as they may not be in the presence of a guardian at the time.

The Terms and Conditions of the App also include clauses for minimum age as well as shared used of mobile phones (Figure 7).

---

<sup>12</sup> <https://support.google.com/googleplay/answer/6209544?hl=en-GB#:~:text=ADULTS%20ONLY%2cor%20gambling%20with%20real%20currency.>



### You must be 16 to accept these terms and to download and use the app

You must be at least 16 years of age to accept these terms and to download and use the app. We are not liable if you allow or enable a person under 16 years of age to install or use the app.

### Only you should use the app and you should not permit anyone else to use your app

---

*Figure 7 Terms and Conditions (extract). <https://protect.scot/terms-and-conditions>*

As it is in the public interest to have a first release of the app available to the public in Scotland as soon as possible -- supporting contact tracing measures to reduce COVID-19 transmission as 'lockdown restrictions' are released -- the app will be released with an age challenge included, asking the user to affirm that they are 16 years of age, or older.

### Why do I have to be at least 16 to use the app?

This is aligned with existing policy for testing and contact tracing, whereby under current arrangements for testing and contact tracing anyone under the age of 16 requires parental consent.

Anyone under the age of 16 will therefore be discouraged from using the app as part of the set up process. However, we are reviewing this to explore whether it might be suitable for people under the age of 16, as we recognise the benefits of the app to younger people. If this position does change, we will communicate this widely.

*Figure 8 FAQs - Why do I have to be at least 16 to use the app? <https://protect.scot/faq>*

It is not perceived that any significant harm will result for individuals younger than 16 years of age using the app, due to the protections built in to protect privacy.

Future versions of the app, where younger people may be able to download it, will require a consultation with the Scottish Government Children and Families Directorate as well as the general public and other groups of interests, to explore options for inclusion of individuals younger than 16 years of age, while meeting the complex competing requirements of inclusion, safeguarding and anonymity. Having





taken advice, the Scottish Government will commit to implementing any agreed modifications in subsequent releases of the app, post-launch.

Inclusion of individuals under the age of 16, at the earliest possible juncture, is a priority for the Scottish Government.

## 6.4 Novelty and Robustness

The Scottish Government is heavily engaged with other countries who are introducing similar apps to help stop the spread of the virus.

Furthermore, the team are in regular contact with Google and Apple, working with these companies to shape the design and functioning of ENS to maximise the value to society and people's health, while protecting the rights to privacy. The use of ENS is considered the best route to a robust working version of the Contact Tracing function. ENS is to provide the ability for apps that implement contact tracing to be functional on both Android and iPhone devices, with the app running in both in the background and foreground; a significant challenge to date. It is expected that ENS will continue optimising, e.g. for better battery efficiency and reduced interference with other Bluetooth peripherals.

The Scottish Government has engaged leading security advisors, and a robust testing plan, including the National Cyber Security Centre, the Scottish Health Competent Authority for compliance with the Security of Network and Information Systems Regulations, independent private sector companies (e.g. penetration testing) and NHS Scotland Information Security Experts, offering expertise in all aspects of the security of the app, including resilience, confidentiality, the integrity of the app and the data.

The scientific community continues to play an important role in the Scottish response to Covid-19. The COVID-19 Data and Intelligence Network has provided expert advice from the research, technology, data and ethics point of view. The Network brings together expertise from across local authorities, health boards, Directors of



Public Health, Health and Social Care Partnerships, Public Health Scotland, Scottish Government, academia and other public bodies.<sup>13</sup>

## 6.5 Accessibility

The app has been carefully designed to be clear and transparent in how it works, to maximise the autonomy of the users (e.g. settings, voluntary input of authorisation codes) and ensuring fully informed consent is sought when required (e.g. automated decision-making).

User Experience of the app has been tested within behavioural studies informing the app flow and content. There is little interaction required for setting up the Contact Tracing function, no identifiable user data input is required, and it can run in the background without user interaction – thus reducing to as much as is possible any barriers to downloading and using the app. Accessibility testing has been included in the QA assessment of the ‘User Interface’ (UI) before the initial app release and will be for subsequent releases (updates). In future, development of Irish language version, and support of other commonly used languages within the country will also be considered.

## 6.6 Consultation and engagement.

As part of this information governance process, from the early stages of the design of the app, consultation has taken place with relevant Scottish groups of interests and advocacy, as well as the relevant supervisory authorities, including:

- The Health and Social Care (Scotland) Public Benefit and Privacy Panel

---

<sup>13</sup> <https://www.gov.scot/publications/coronavirus-19-covid-19-surveillance-response/pages/5/>



- The Scottish Privacy Forum and CRIP (Centre for Research into Information, Surveillance & Privacy)<sup>14</sup>
- The Open Rights Group
- The Data ethics and public engagement subgroup of the COVID-19 Data and Intelligence Network
- Information Commissioner's Office

The purpose of these consultations was to gather views, perspectives, and experiences from experts, and members of the public, on a range of interrelated issues.

From the app development perspective, issues such as privacy, appropriate use of data, cybersecurity, data accuracy, and accessibility were explored.

From a societal and ethical perspective, issues such as social inequalities, ethical implications, engagement with health services, and user expectations, needs and engagement, were explored.

As a result a “Digital and Data Ethics” summary was prepared (APPENDIX C – Digital and Data Ethics Summary) illustrating the scope and impact of the app in society, the core ethical principles:

- Beneficence – those are the core benefits the app
- Non-maleficence – these were considerations illustrating how the app causes no-harm to individuals or society
- Autonomy – considerations to ensure people have control over the app functionality, their data and their privacy.

---

<sup>14</sup> <http://www.crisp-surveillance.com/scottish-privacy-forum>

- Fairness and compliance – considerations to ensure the app is fair for the people of Scotland and complies with legislation, such as data protection but also medical devices regulations.

The following specialist assessments were also conducted:

- Medical Devices Regulations
- Data Protection (UK)\* and Common Law Duty of Confidentiality
- Human Rights, Fairer Scotland Duty and Equality\*
- Children Rights and Wellbeing\*

The asterisk indicates an assessment that has been or will be published online as soon as possible, in line with the transparency promise for the Protect Scotland App. Updates and links will be provided here: <https://protect.scot>

#### **6.6.1 Direct engagement with data subjects.**

Alliance Scotland supported consultation with members of their citizen engagement group; people were invited to provide feedback on the clarity of the Privacy Notice as well as their privacy concerns. The questionnaire used to gather feedback is available in APPENDIX A – Citizen engagement.

A Creative Testing exercise using qualitative research was also conducted, which included testing through focus groups and depth interviewing with a sample of Smartphone users in Scotland.

This public engagement aimed to:

- identify the best ways to encourage data subjects to download the app, highlight any barriers or drivers around downloading the app which could be addressed.
- Identify any areas of concern and possible optimisation on the language used or the user journey

- Understand views of the intended functionality of the app, and whether any other functions would be desirable at a future stage for either the Test & Protect App or Test & Protect overall
- Understand how clearly the privacy notice explained the processing and to identify ways to improve transparency in general, but also the language in particular.

Participants recruited from across Scotland from both urban and rural locations & included a mix of gender. Over 50 people took part across the various public engagement initiatives.

Almost all participants had used other apps before. People appreciated a familiar logo on the app, star ratings (reviews) and fully integrated technology so they didn't have to spend time inputting information. It was valued a clear and unique name for the app to ensure they didn't download the wrong app.

Most felt that apps can be secure (e.g. well known banks) but concerns were more in relation to other apps where they had to type in a lot of personal information.

Lack of storage space in their phones, fear about hidden costs were also common concerns, along with the following when downloading app:

- Signing up to something they have to pay for
- Doing something wrong
- Data harvesting (particularly location data)
- Battery drainage
- Storage space
- Scams – stealing data, card/bank details, etc.
- Viruses
- Receiving junk emails and unwanted targeted ads
- Getting hacked
- Knowing how your data is going to be used and how long it will be kept



Older respondents were particularly concerned about data security, viruses and hacks.

Younger respondents were more likely to mention the cost, storage space, and time-consuming signup procedures.

Although some issues were identified around the technical language used and clarity on how the app works, most were forgiving due to the importance of the need to suppress the virus; however, this feedback was taken into account and embedded the app as part of the privacy by the design process.

With regards to clarity within the privacy notice, the majority of the respondents indicated that, after reading the privacy notice, they could identify:

- what organisations are involved and what their role is regarding the app
- what the contact details for data protection officer are
- what the purposes of the app are
- what data is used by the app
- whether health data is used or not
- how your personal data, phone number and IP Addresses are obtained
- why it is necessary to process your data in the ways described
- what the legal basis for this is
- where your data goes, who has access to your data, and whether your data goes outside the UK
- for how long your data is held and when it is deleted
- what your rights are and how to exercise them in the app
- what to do if you don't want the app anymore
- how to lodge a complaint with the Information Commissioner's Office
- the automated decisions made by the app and how to contest automated decisions (e.g. by calling to a helpline etc.)

People indicated that the length of the privacy notice (as initially designed) was off-putting, but appreciated the level of detail and the legal requirement to cover various aspects; therefore the online version has been condensed, offering options to navigate to specific sections and is accompanied with a series of questions and answers to expand on areas of interest, at the discretion of the data subject, without compromising the essential elements of the privacy notice.



Feedback from specific groups, including people with dementia wasn't conclusive and whether some people appreciate adaptations to their needs, other preferred

## 7 Compliance with data protection legislation and other regulatory guidance

### 7.1 Legal basis for the processing.

#### Personal Data:

- **Mobile phone number**
- **Estimated date of infection**
- **Authorisation code**
- **Diagnosis keys**
- **IP address**
- **Your confirmation of app use**

Data Controller	Legal basis
<b>Scottish Government</b>	<ul style="list-style-type: none"> <li>• Necessary for performance of a task carried out in the public interest on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 6(1)(e)).</li> <li>• Necessary for reasons of substantial public interest for statutory and Government purposes on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 9(2)(g)).</li> <li>• Necessary for reasons of public interest in the area of public health on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 9(2)(i)).</li> <li>• Necessary for scientific research or statistical purposes in the public interest (GDPR Art 9(2)(j)).</li> </ul>
<b>NHS National Services Scotland</b>	<ul style="list-style-type: none"> <li>• Necessary for performance of a task carried out in the public interest on the basis of The National Health Service (Functions of the Common Services Agency) (Scotland) Order 2008 Section 2 (Functions of the Agency) (duty to provide services in support of the functions of Scottish Ministers, Health Boards or Special Health Boards) (GDPR Art 6(1)(e)).</li> <li>• Necessary for reasons of public interest in the area of public health (GDPR Art 9(2)(i)).</li> </ul>
<b>Public Health Scotland</b>	<ul style="list-style-type: none"> <li>• Necessary for performance of a task carried out in the public interest on the basis of Public Health Scotland Order 2019 section 4 (Functions of the Board, in particular (d) the protection of public health including those specified in section 1 of the Public Health etc. (Scotland) Act 2008 (duty of Scottish Ministers to protect public health)) and The Health Protection (Coronavirus) (International Travel) (Scotland) Regulations 2020, (Part 5 (Information Sharing – Power to use and disclose Information) (GDPR Art 6(1)(e)).</li> </ul>



**Personal Data:**

- **Exposure notification**

Data Controller	Legal basis
<b>Scottish Government</b>	<ul style="list-style-type: none"> <li>• Necessary for the performance of a task carried out in the public interest on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 6(1)(e))</li> <li>• Explicit consent (GDPR Art 9(2)(a))</li> <li>• Necessary for reasons of substantial public interest for statutory and Government purposes on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 9(2)(g)).</li> <li>• Necessary for reasons of public interest in the area of public health on the basis of The Public Health etc. (Scotland) Act 2008 section 1 (Duty of Scottish Ministers to protect public health) (GDPR Art 9(2)(i)).</li> <li>• Necessary for scientific research and statistical purposes in the public interest (GDPR Art 9(2)(j)).</li> </ul>
<b>NHS National Services Scotland</b>	<ul style="list-style-type: none"> <li>• Necessary for performance of a task carried out in the public interest on the basis of The National Health Service (Functions of the Common Services Agency) (Scotland) Order 2008 Section 2 (Functions of the Agency) (duty to provide services in support of the functions of Scottish Ministers, Health Boards or Special Health Boards) (GDPR Art 6(1)(e)).</li> <li>• Explicit consent (GDPR Art 9(2)(a)).</li> <li>• Necessary for scientific research and statistical purposes in the public interest (GDPR Art 9(2)(j)).</li> </ul>
<b>Public Health Scotland</b>	<ul style="list-style-type: none"> <li>• Necessary for performance of a task carried out in the public interest on the basis of Public Health Scotland Order 2019 section 4 (Functions of the Board, in particular (d) the protection of public health including those specified in section 1 of the Public Health etc. (Scotland) Act 2008 (duty of Scottish Ministers to protect public health)) and The Health Protection (Coronavirus) (International Travel) (Scotland) Regulations 2020, (Part 5 (Information Sharing – Power to use and disclose Information) (GDPR Art 6(1)(e)).</li> <li>• Explicit consent (GDPR Art 9(2)(a)).</li> <li>• Necessary for scientific research and statistical purposes in the public interest (GDPR Art 9(2)(j)).</li> </ul>

**7.1.1 Duty of Confidentiality.**

The app is voluntary to use. A number for features allows you to control what the app can do, in particular:





- The 'App settings' give people the ability to delete the app and any information stored on the phone while using the app.
- People can decide if you want to allow 'COVID-19 Exposure Notification Services' on your phone.
- People can also choose to receive notifications when they have been exposed to someone who has tested positive for COVID-19. People can turn on and off this functionality in the notifications settings of their mobile phone any point in time.

By downloading the app, and using the app with their preferred settings and having to input voluntarily 'Authorisation Codes' to upload 'Diagnosis Keys', there is an understanding that people agree with the terms and conditions of the app and consent is given from Duty of Confidentiality law point of view.

### 7.1.2 Automated decision-making

Exposure notifications: the generation of exposure notifications advising you to self-isolate is an automated process, not involving a human. This is carried out on the basis of the consent the App User provided when started using the app.

The exposure notification includes the date of potential exposure. Still, it does not include information about where and with whom the potential exposure took place, as we have no way of knowing this.

The App User will receive an exposure notification if any of the random IDs stored on their device matches with a diagnosis key released by another app user by inserting their authorisation code into their device after that app user has received a positive COVID-19 test result.

The app tries to match the random IDs on your device with the diagnosis keys on the app server every 2 hours. The exposure notification means that your device has been within 2 meters of that other app user's device for at least 15 minutes within a 14 days period during which that other app user could have passed the virus on to



the App User. The 14 day period from which the diagnosis keys are taken is the 14 days immediately prior to the authorisation code being inserted.

The app will advise the App User to self-isolate in line with current guidelines, and signpost you to further information. Although recommended, the decision on whether or not to self-isolate is ultimately the App User's.

If after reading the additional information provided via the NHS Inform website, the App User wishes to discuss the advice to self-isolate and its implications, they can call the National Helpline (0800 028 2816) who can help you to understand the message. If they think the advice to self-isolate is incorrect, they have the right to challenge it by calling the National Helpline. If they have tested positive, they can discuss the notification with a contact tracer to understand the implications.

The App User can disable exposure notifications from the app settings at any time and uninstall the app from their device at any time. However, doing so will prevent them from receiving exposure notifications.

### **Automated and semi-automated processing**

When authorisation code is inserted, the device sends the diagnosis keys to the app server using the IP address of the device and these are held on the server anonymously to allow other app users' devices to search for a match. The processing does not require consent as it is not based solely on automated processing as app users are required to take action to insert authorisation codes into the app.

Processing of anonymised random IDs: the processing of anonymised random IDs as a result of close proximity with other app users is also an automated process. To work, the app requires that location services are switched on on Android phones, but the app does not use GPS location services or Google location services to track your movements. You can stop this processing of anonymised random IDs by disabling the Bluetooth feature of your device (or location on Android phones).

The processing does not require consent as the random IDs are anonymised. The App User also can delete the anonymised random IDs stored on their device using the settings and uninstall the app from their device at any time.

### **Storage and access to information on your device**

The app stores and accesses information on your device (for example, the diagnosis keys from your device are provided to the app server if you enter an authorisation code). For the purposes of the Privacy and Electronic Communications Regulations (PECR) 2003, such storage and access are strictly necessary for the service provided by the app.

The app also complies with PECR rules as follows:

- The app does not use cookies.
- The app does not generate unsolicited marketing calls, emails text or faxes.
- The app keeps all communication services secure.
- The app does not store IP addresses.
- The data processed by the app is strictly the minimum necessary.
- Metrics constructed by the app are anonymous and aggregated. This data is also essential to monitor the efficacy of the app and to obtain CE marking as required by the Medical Devices Regulations and MHRA guidance.

#### **7.1.3 Medical devices regulations.**

The functionality of the app is borderline with the definition of software as a medical device category I. In order to err in the side of caution, the app will search for CE marking accreditation and will follow the MHRA guidance.

The app will be launched under the six month MHRA 'Exemption from device regulation during COVID-19', however, for continuity of the app after the six month period, it is essential that sufficient anonymous metrics are collected to demonstrate the efficiency of the app primary function, and for attaining CE accreditation.



App users are explicitly informed of the scope of the metrics collected, and the purpose of collecting that data, during the onboarding process.

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.”

## 7.2 Data Protection rights

There are no fundamental changes to the data protection rights. The Data Protection Act 2018 and GDPR provide individuals with a number of rights relating to their personal data:

*Table 5 Data protection rights for app users.*

Your data protection right	How to exercise your right
<b>The right to access your personal information.</b>	Since only very limited personal information is retained in a short term and temporary manner, it would not be possible to comply with this request.



Your data protection right	How to exercise your right
<p><b>The right to have personal information rectified if it is inaccurate or incomplete.</b></p>	<p>If you suspect your mobile number used to issue your authorisation code to you or your estimated date of infection are incorrect, please contact the NHS Scotland National Contact Tracing Centre</p> <p>Since only very limited personal information is retained within the app or the server and such information is retained in a short term and temporary manner, it would not be possible to comply with this request</p> <p>You have the right to contest and seek rectification of your exposure notification</p>
<p><b>The right to have personal information erased and to prevent processing.</b></p>	<p>If you want to delete the anonymous random IDs stored on your device you can do so using the device settings. You can also select the 'Leave' function in the settings and/or uninstall the app at any time</p> <p>Since only very limited personal information is retained within the app server and such information is retained in a short term and temporary manner it would not be possible to comply with this request</p>
<p><b>The right to 'block' or suppress processing of personal information.</b></p>	<p>Using settings you can disable exposure notifications and the collection of anonymous random IDs by turning off Bluetooth on your device. You can delete the anonymous data from your device at any time</p> <p>You can also select the 'Leave' function in the settings and/or uninstall the app at any time</p> <p>You can decide not to insert the authorisation code into the app to release the diagnosis keys</p> <p>Other than the above measures, since only very limited personal information is retained and such information is retained in a short term and temporary manner, it would not be possible to comply with this request</p>



Your data protection right	How to exercise your right
<p><b>The right to portability.</b></p>	<p>Since only very limited personal information is retained in the app server and such information is retained in a short term and temporary manner, it would not be possible to comply with this request</p> <p>app functionality does not allow porting the anonymous random IDs from your device</p>
<p><b>The right to object to the processing.</b></p>	<p>If you want to delete the anonymous data stored on your device you can do so using the device settings. You can also select the 'Leave' function in the settings and/or uninstall the app at any time.</p>
<p><b>Rights in relation to automated decision making and profiling.</b></p>	<p>The decision on whether or not to self-isolate is ultimately yours. If after reading the <a href="#">additional information</a>, you wish to discuss the advice to self-isolate and its implications, you can call the National Helpline (0800 028 2816) or your existing contact tracer to understand the exposure notification and to make an informed decision as to whether to self-isolate</p> <p>You also have the right to contest and seek rectification to the automated advice to self-isolate by calling the NHS 24 Helpline</p> <p>Using settings you can disable exposure notifications and the collection of anonymous random IDs by turning off Bluetooth on your device. You can delete the anonymous random IDs from your device at any time</p> <p>You can also select the 'Leave' function in the settings and/or uninstall the app at any time</p>

### 7.3 Compliance with data protection principles.

This Data Protection Impact Assessment is not focused on risks and impact for the data controllers but mainly on app users, as the data subjects, and other citizens.



### 7.3.1 Principle 1 – fair and lawful, and meeting the conditions for processing

Article 5(1) of the GDPR says:

“1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness, transparency’)”

*Table 6 Statement of compliance with Principle 1*

#### Lawful, fair and transparent processing

##### Lawfulness –

- ✓ Scottish Government, Public Health Scotland and NHS National Services Scotland, have identified an appropriate lawful basis (or bases) for the processing as well as a condition for processing health data (special categories) (refer to section 7.1).
- ✓ None of the data controllers, data processor or their subcontractor do anything generally unlawful with the data.

##### Fairness

- ✓ We (the data controllers) have considered how the processing may affect the individuals concerned and can justify any adverse impact (refer to section 8
- ✓ Risks to data subjects rights and freedoms.).
- ✓ We only handle people’s data in ways reasonably expected; the app, the privacy notice and this document explain in detail how the data is handled.
- ✓ We do not deceive or mislead people when we process their personal data.

##### Transparency

- ✓ Scottish Government, as well as Public Health Scotland and NHS National Services Scotland have been open and honest, and comply with the transparency obligations of the right to be informed.



### 7.3.2 Principle 2 – Purpose limitation

Article 5(1)(b) says:

“1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.”

Table 7 Statement of compliance with Principle 2

Purpose limitation
<ul style="list-style-type: none"> <li>✓ Scottish Government has clearly identified the purposes for processing the data in this DPIA (refer to section 5.2.1 Purposes for which personal data is used.) and the Privacy Notice.</li> <li>✓ We have documented those purposes in this DPIA.</li> <li>✓ We include details of our purposes in our privacy information for individuals.</li> <li>✓ We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.</li> <li>✓ Scottish Government will not be able to use personal data for any other purposes since personal data is not stored in the App.</li> </ul>

### 7.3.3 Principle 3 – adequacy, relevance and data minimisation

Article 5(1)(c) says:

“1. Personal data shall be:

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)”

Scottish Government, Public Health Scotland and NHS National Health Services have put in place a series of measures, as described in Table 8 Statement of compliance with Principle 3, to ensure that the personal data being processed is:

- adequate and otherwise sufficient to properly fulfil the stated purpose of the app;
- relevant and pertinent to that purpose; and





- limited to what is necessary (not hold more data than what is need for that purpose).

Table 8 Statement of compliance with Principle 3

Adequacy, relevance and data minimisation measures
<ul style="list-style-type: none"><li>✓ The app only processes the minimum personal data that is essential for the specified purposes. Details of what data is necessary are described in Section 5.2 (Personal data)</li><li>✓ The data described in this DPIA is sufficient to properly fulfil the purposes of the app.</li><li>✓ The data minimization applied to this app by design is an excellent model by:<ul style="list-style-type: none"><li>○ collecting only the minimum data required (only personal data collected is the mobile number and the relevant date of infection)</li><li>○ using only the minimum data for the shortest period of time, therefore, removing data items that can be associated to an app user immediately after use (e.g. IP addresses)</li><li>○ not storing any personal identifiable data</li><li>○ finding creative ways of fulfilling a purpose with alternative non personal data (e.g. using anonymous keys wherever possible, not collecting location data, keeping the SMS Job Ids only for reconciliation purposes)</li></ul></li><li>✓ The culture across the app team, from leadership to development, implementation and information governance is extremely focused on data minimization by design.</li><li>✓ There are processes in place to ensure that only essential personal data is processed. The rationale has been discussed with independent groups (refer to 6.6 Consultation and engagement.)</li></ul>

### 7.3.4 Principle 4 – accurate, kept up to date, deletion

Article 5(1)(d) says:

“1. Personal data shall be:

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)”



Scottish Government, Public Health Scotland and NHS National Health Services have taken all reasonable steps, as described in Table 9 to ensure that:

- the personal data held is not incorrect or misleading as to any matter of fact,
- the personal data is kept updated as appropriate,
- incorrect or misleading data is corrected or erased as soon as possible,
- any challenges to the accuracy of personal data are carefully consider.

Table 9 Statement of compliance with Principle 4

Data accuracy
<ul style="list-style-type: none"><li>✓ We ensure the accuracy of any personal data created by the App.</li><li>✓ We have appropriate processes in place to check the accuracy of the data collected by the app, and we record the source of that data.</li><li>✓ We have appropriate information in place to ensure app users understand the terms and conditions of the app, and for using the app and their mobile phones responsibly and effectively. The ENS will record the fact the phone has been in close proximity with other app users, regardless who is carrying the phone at that time. This is factual data.</li><li>✓ The app doesn't store personal identifiable data, therefore, there will not be a requirement to keep data up to date, however, we have a process in place to identify when mobile numbers provided by the CMS need to be updated by the CMS.</li><li>✓ We keep records that identify SMS jobs that used invalid or incorrect mobile numbers.</li><li>✓ We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. Refer to Section 7.2 Data Protection rights.</li><li>✓ We have processes in place to periodically review the quality of the data (mobile numbers) sourced by the National Contact Tracing Centre (CMS). There is a reconciliation process to monitor that SMS have successfully reached the App User. In the event of high volumes of SMS errors being returned by the Gov.UK Notify service, this will be addressed jointly with the National Contact Tracing Centre.</li><li>✓ We have a strong communications campaign to ensure the public understand the importance of using their mobile phones and the App</li></ul>



responsibly and effectively in order to maximise the benefit for themselves and others.

- ✓ We have had weekly meetings with the Information Commissioner’s Office and we have discussed this issue. We are satisfied we are applying all reasonable measure to minimize the impact; we also work closely with the National Contact Tracing Center to ensure the source of data has the highest feasible quality

### 7.3.5 Principle 5 – kept for no longer than necessary, anonymisation

Article 5(1)(e) says:

“1. Personal data shall be:

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’)”

Table 10 Statement of compliance with Principle 5

Anonymisation and retention.
<ul style="list-style-type: none"> <li>✓ No personal data is stored by the App.</li> <li>✓ We carefully consider if personal data needs to be held and can justify how long we keep personal data (e.g. SMS jobs are held for 7 days within the Gov.UK Notify service because this is an external very secure service that only applies a standard data retention policy to all customers (only government bodies in the UK and NHS) using their service. Their data retention policy is 7 days, and cannot be customised for App. The data is encrypted and is not visible by any users of the Gov.UK Notify system.</li> <li>✓ The policy for the App is to delete any personal data straight after use (e.g. after sending the SMS – typically within 2 hours of generating the SMS, after IP Addresses reach destination – typically within seconds of sending data to the network).</li> <li>✓ The app regularly anonymise personal data when we no longer need it. For further details, refer to Section 5.2.2 (Data minimisation and anonymisation.) and Section 5.2.3 (Data retention)</li> <li>✓ Since the App doesn’t store personal data, it won’t be applicable to have processes to comply with individuals’ requests for erasure (see 7.2 Data Protection rights – for further details)</li> </ul>



- ✓ We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes. refer to the following sections:
  - 4.2 Reporting metrics.
  - 5.2 Personal data (Metric data) Reporting metrics.
  - 7.1 Legal basis for the processing.

### 7.3.6 Principle 6 – Information Security.

Article 5(1)(f) of the GDPR concerns the ‘integrity and confidentiality’ of personal data. It says that personal data shall be:

'Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'

Scottish Government, Public Health Scotland and NHS National Health Services have taken all reasonable steps, as described in Table 11 to ensure that appropriate security measures are in place to prevent the personal data processed by the app being accidentally or deliberately compromised.

While information security is sometimes considered as cybersecurity (the protection of your networks and information systems from attack), it also covers other things like physical and organisational security measures.

A full description of the technical and security measures has been documented in the System Security Policy (SSP) for the app.

Some of the technical and organisational security information is available here: <https://github.com/NES-Digital-Service/protect-scotland>; however, Security Policies are commonly exempt from Freedom of Information, as they may disclose specific vulnerabilities that can be exploited by cybercriminals. The FOI (Scotland) Act exempts information if its disclosure is likely to prejudice the prevention of crime (including cybercrime).



The Information Security Risk Assessment has analysed 25 threats taken from the ISO 27799<sup>15</sup> Annex A – “Threats to health information security”.

The technical and organisational security measures implemented to mitigate these risks are considered appropriate for the level of risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons<sup>16</sup>.

Table 11 Statement of compliance with Principle 6

Information Security (Technical and organisational measures)
<ul style="list-style-type: none"><li>✓ We undertake an analysis of the risks presented by the App processing, and use this to assess the appropriate level of security we need to put in place</li><li>✓ We implement measures that adhere to the National Cyber Security Centre principles and guidelines, the Security of Network and Information Systems (NIS) Regulations, Medical Devices regulations and the NHS Information Security Policy Framework.</li><li>✓ We ensure that any data processor we use also implements appropriate technical and organisational measures.</li><li>✓ When deciding what measures to implement, we take account of the state of the art and costs of implementation, but also the opportunities and the importance of the app in dealing with the COVID-19 pandemic.</li><li>✓ We have an information security policy and take steps to make sure the policy is implemented.</li><li>✓ We have additional policies different elements of the App and ensure that controls are in place to enforce them.</li><li>✓ We make sure that we regularly review our information security policies and measures and, where necessary, improve them.</li></ul>

---

<sup>15</sup> ISO 27799:2016 — Health informatics — Information security management in health using ISO/IEC 27002.

<sup>16</sup> GDPR, Art. 32 (Security of the processing) provides a perspective to the reasonability of the security measures to be required.



- ✓ We have put in place technical controls such as those specified by established frameworks like Cyber Essentials.
- ✓ We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- ✓ We use encryption, anonymisation and pseudonymisation where it is appropriate to do so.
- ✓ We understand the requirements of confidentiality, integrity and availability for the personal data we process.
- ✓ We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- ✓ We conduct regular testing, including Penetration Testing, and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement.
- ✓ All data stored in 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 the App servers. The App does not access GPS functionality or any form of location data from your phone.
- ✓ The SMSs that are sent via Gov.UK Notify are also encrypted and secure service for government use. This service complies with the National Cyber Security Centre (NCSC) Cloud Security Principles. Further security information is available [here](#).

## 7.4 International transfers.

No personal data is transferred outside the UK. All data processing will be subject to Data Protection (UK) legislation.

Once the Federated Interoperability server is implemented, anonymous diagnosis keys will be shared. This document and the privacy notice will be updated to reflect this use of the anonymous data.



## 8 Risks to data subjects rights and freedoms.

This section is in response to the guidelines on Data Protection Impact Assessments<sup>17</sup> to determine whether the processing is “likely to result in a high risk”, primarily as a result of the introduction of new technologies for contact tracing, which includes some features of automated decision-making (refer to section 7.1.2 Automated decision-making).

The purpose of this section is to determine when the processing operations of the App may result in a high risk to the rights and freedoms of people, and thus takes their perspective, as is the case in specific fields (e.g. societal security).

Conversely, risk management in other fields (e.g. information security) is focused on the organisations (the data controllers). The Information Security Risk Assessment referred to in section 7.3.6 (Principle 6 – Information Security.) is focused on the organisation. It has been used to inform the risks to the rights and freedoms of people included in this section.

The following separate specialist assessments have also been used to inform the level of risk and countermeasures:

- Medical Devices Regulations
- Data Protection (UK)\* and Common Law Duty of Confidentiality
- Human Rights, Fairer Scotland Duty and Equality\*
- Children Rights and Wellbeing\*

The asterisk indicates an assessment that has been or will be published online as soon as possible, in line with the transparency promise for the Protect Scotland App. Updates and links will be provided here: <https://protect.scot>

---

<sup>17</sup> WP 248 - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679.



A summary of the scoring system used for risks in the document is illustrated in Table 12. Further details are available in PPENDIX D – Risk scoring system.

Table 12 Risk scoring system (source: The Scottish Information Sharing Toolkit<sup>18</sup>)

**Risk Assessment Matrix**

Likelihood		Consequence				
		Negligible	Minor	Moderate	Major	Extreme
		1	2	3	4	5
Almost certain	5	LR 5	MR 10	HR 15	HR 20	HR 25
Likely	4	LR 4	MR 8	MR 12	HR 16	HR 20
Possible	3	VLR 3	LR 6	MR 9	MR 12	HR 15
Unlikely	2	VLR 2	LR 4	LR 6	MR 8	MR 10
Remote	1	VLR 1	VLR 3	VLR 3	LR 4	LR 5

■ Very Low Risk (VLR)   
 ■ Low Risk (LR)   
 ■ Moderate Risk (MR)   
 ■ High Risk (HR)

<sup>18</sup> <https://www.informationgovernance.scot.nhs.uk/istresources/>





## R 1. The overall risk to rights and freedoms position

The following sections analyse the risk to the rights and freedoms of natural persons, with varying likelihood and severity.

The control measures described in this document reduce the likelihood and potential impact to data subjects, to ensure the use of the app cannot lead to physical, material or non-material damage. In particular, risks of discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality, unauthorised reversal of pseudonymisation have been mitigated.

No other significant economic or social disadvantages have been identified.

The overall risk of the processing to the rights and freedoms of the data subjects is considered **low**.

## R 2. Risk: Unfair and non-transparent processing.

Risk	<b>Unfair and non-transparent processing.</b>
Impact	<p>Significant adverse impact to people’s rights and freedoms as a result of the processing of personal data (e.g. unfair frequent requirement to self-isolate, loss of income and missed entitlement to sick pay or other benefits).</p> <p>Data may be inadvertently collected about children in the app. Children may receive notifications of exposure and cause</p>
Privacy by design and by default notes.	<p><b>Fairness</b></p> <ul style="list-style-type: none"> <li>✓ We have considered how the processing may affect the app users concerned and we have taken measure to prevent the risk of unfair processing of data (e.g. no retaining personal data beyond the minimum necessary, ensuring the app meets the requirements of notification for sick pay purposes, ensuring the app is entirely voluntary, not using location data and not tracking people’s movements or adherence to self-isolation, etc.)</li> <li>✓ We have consulted with independent groups and the general public</li> <li>✓ We only handle people’s data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.</li> <li>✓ We have included age controls during on-boarding process in the app (limited since the app doesn’t have a way to verify age). Clear FAQs for parents and app users. User must agree to Ts&amp;Cs (including age</li> </ul>



		requirements). People under 16 will not receive Authorisation Codes necessary for sharing Diagnosis Keys.		
		<ul style="list-style-type: none"> <li>✓ We are transparent with the public and the code is in the public domain for independent scrutiny.</li> <li>✓ There has been a rigorous process to test and validate the accuracy and effectiveness of the app, and the clarity of the communications with the public.</li> <li>✓ We are open and honest, and comply with the transparency obligations of the right to be informed (see <a href="https://protect.scot/privacy-policy-app">https://protect.scot/privacy-policy-app</a> and <a href="https://protect.scot/how-we-use-your-data">https://protect.scot/how-we-use-your-data</a>).</li> </ul>		
Unmitigated risk score		Further mitigation controls	Residual risk score	
Likelihood	Unlikely	None.	Likelihood	Remote
Impact	Minor		Impact	Minor
Score	Low Risk		Score	Very Low Risk

### R 3. Risk: Personal data used for other purposes.

Risk	<b>Personal data used for other purposes.</b>			
Impact to the data subjects	Negligible.			
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ The app does not store personal data, therefore is not possible to use it for any further purposes.</li> <li>✓ It is very unlikely and impractical that Personal data (SMS) retained for 72hrs within the Gov.UK Notify service could be required for other purposes (e.g. law enforcement).</li> <li>✓ Any proposed changes to the app, included extended use of any data, are subject to a rigorous Change Management and Information Governance Processes and transparency.</li> </ul>			
Unmitigated risk score		Further mitigation controls required	Residual risk score	
Likelihood	Unlikely	None	Likelihood	Remote
Impact	Minor		Impact	Negligible
Score	Low Risk		Score	Very Low Risk

### R 4. Risk: Exercise of data protection rights.

Risk	<b>People cannot exercise their data protection rights.</b>			
Impact to the data subjects	Unsatisfactory citizen experience with the app with no clinical outcome/harm).			
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ App includes functionality to allow data subjects to exercise their data protections righthst directly within the app interface including:</li> <li>✓ Voluntary download</li> <li>✓ Requires authorization code from the user in order to upload diagnosis keys</li> <li>✓ Customization of settings (e.g. notifications, ENS)</li> <li>✓ Data deletion (Leave option and clearing exposure notifications)</li> </ul>			



		<ul style="list-style-type: none"> <li>✓ The app does not store personal data, which minimises significantly the scope of applicability of data protection data rights.</li> <li>✓ Alternative process via Data Protection Officers</li> <li>✓ Information about how to exercise their rights is available in other languages and formats by request. Details are available in the privacy notice.</li> </ul> <p><b>(Refer to section 7.2 Data Protection rights)</b></p>		
Unmitigated risk score		Further mitigation controls required	Residual risk score	
Likelihood	Unlikely	None	Likelihood	Remote
Impact	Minor		Impact	Negligible
Score	Low Risk		Score	Very Low Risk

### R 5. Risk: False positive alerts.

Risk	<b>People may receive incorrect exposure notifications, and be asked to self-isolate when is not required.</b>				
Impact to the data subjects	Adverse impact in freedoms of the individual (isolation) for 2 weeks at a time, with potential accumulative effect. Impact on family and work life. Financial loss. Variable psychological impact.				
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ App includes controls to avoid data pollution, e.g. functionality to ensure only people over 16 who have tested positive from COVID-19 and receive the authorization codes to upload their diagnosis keys.</li> <li>✓ Network and security measures are put in place to block attacks of scale</li> <li>✓ Ensure device integrity checks are first performed by the app during the on boarding, and to ensure for all traffic to the app backend is protected via this means</li> <li>✓ Communications plan and Ts&amp;Cs remind people that they should take suitable precautions to protect their mobile device to avoid their devices recording incorrect exposure keys.</li> <li>✓ Use ENS to benefit from extensive capability of Google and Apple to do extensive testing (e.g. Bluetooth technology, power measurement, false positives)</li> <li>✓ Create a well-designed communication plan to ensure those that may be susceptible to causing false positives understand what they can do (e.g. turn off Contact Tracing while other measures in place can produce non genuine close contact readings – wall/glass, etc.)</li> <li>✓ Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for over reporting of close contacts</li> <li>✓ Helpline to challenge exposure notification alerts (as an automated decision)</li> </ul>				
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Unlikely
Impact	Moderate			Impact	Moderate
Score	Moderate			Score	Low Risk



### R 6. Risk: False negative alerts.

Risk		<b>People who have been exposed do not receive an exposure notification (false negative)</b>			
Impact to the data subjects		People who have been in close contact are not identified and asked to self-isolate, increasing their own level of exposure and potentially spreading the virus to their households, at work and others.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Ensure app is used to augment the existing contact tracing strategy</li> <li>✓ Engage in comprehensive testing with the app and in a Scottish environment</li> <li>✓ Use ENS to benefit from extensive capability of Google and Apple to do extensive testing</li> <li>✓ Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for under reporting of close contacts</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Unlikely
Impact	Major			Impact	Moderate
Score	Moderate			Score	Low Risk

### R 7. Risk: Unlawful international data transfers.

Risk		<b>Risk that personal identifiable data will be transferred to a country with less protections to people's rights and freedoms.</b>			
Impact to the data subjects		Limited potential for misuse of SMS data containing mobile number, authorization code and relevant date of infections. Potential data pollution.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Data minimization</li> <li>✓ Anonymisation at first opportunity</li> <li>✓ Encryption of data</li> <li>✓ App does not store personal identifiable data</li> <li>✓ Data processing agreements to be put in place with all data processors involved in the app, which restricts data transfers and storage to the EEA or other locations with which the EEA have approved mechanisms.</li> <li>✓ Information security controls in line with National Cyber Security Centre guidelines.</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Remote
Impact	Minor			Impact	Negligible
Score	Low risk			Score	Very Low risk

### R 8. Risk: Interrupted cross-border contact tracing.

Risk		<b>Risk that the processing is interrupted when people work and live across various country borders or travel to abroad.</b>	
Impact to the data subjects		Unsatisfactory experience using the App. Failure to record exposure, send exposure notifications. Failure to help stopping chain of infection.	



Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Ensure that the app is to augment the existing contact tracing and testing strategy in Scotland and that under this umbrella, of wider operational cooperation and coordination, that app interoperability is considered.</li> <li>✓ Ensure that engagement with the UK (and other countries) specifically in regards with wider contact tracing and testing operational coordination and cooperation is pursued.</li> <li>✓ Ensure the Protect Scotland app can be installed by people in the Scottish borders</li> <li>✓ Engage with the UK and other countries in relation to cross border app interoperability</li> <li>✓ Engage with Google and Apple in relation to cross border interoperability</li> <li>✓ Engage at an EU level in regards cross border interoperability</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Likely	None		Likelihood	Unlikely
Impact	Moderate			Impact	Moderate
Score	Moderate Risk			Score	Low risk

### R 9. Risk: excessive personal identifiable data

Risk	<b>Risk that irrelevant or excessive personal identifiable data is processed by the app.</b>				
Impact to the data subjects	Unfair processing, restrictions to the privacy of the individual (e.g. identity theft, reversal of anonymous data) and restrictions to people's freedoms and rights (e.g. no longer voluntary or with more limited choices)				
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ Ensure the guidelines for proximity apps are carefully assessed</li> <li>✓ Ensure that features are clearly aligned with the purpose of the app being a COVID-19 response app</li> <li>✓ Ensure the SLGW for the App and the Information Governance processes scrutinise the data and functionality of the app in line with the data protection principles and data ethics principles</li> <li>✓ Engage with independent experts, including, privacy groups, Caldicott Guardians and ethics advisors to inform decisions</li> <li>✓ Ensure that the app's features can be used independent of each other and that this is clear to the users</li> </ul>				
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Likely	None		Likelihood	Unlikely
Impact	Major			Impact	Minor
Score	High Risk			Score	Low risk

### R 10. Risk: reversal of anonymous data.

Risk	<b>Risk that anonymous data can be reversed, identify individuals and expand use of data for unintended purposes.</b>				
Impact to the data subjects	Unfair processing, restrictions to the privacy of the individual and restrictions to people's freedoms and rights (e.g. identify and track				



		individuals, financial loss ). Show COVID-19 status of the data subject. Undermine confidence in the app.	
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Transparency with regards to what data is processed, and when the data is anonymized (timelines).</li> <li>✓ All metric data must be anonymised (or anonymised at the earliest processing point - noting IP address as per DPIA) and carefully reviewed for any re-identification potential. Do not pass IP addresses from networking layer to application layer in app backend.</li> <li>✓ App designed to avoid showing health status of the App user.</li> <li>✓ Release source code to ensure transparency of processing. Open source code for inspection.</li> <li>✓ Ensure app does not use 3rd party analytics tools to gather metric data, which could unintentionally or otherwise be recombined to re-identify people</li> <li>✓ Ensure app governance appropriately reviews and protects against this re-identification risks.</li> <li>✓ Adopt a decentralised approach for the Contact Tracing function</li> <li>✓ Do not use location services for Contact Tracing</li> <li>✓ Adopt the Google and Apple API implementation, which is receiving significant worldwide analysis from privacy experts</li> <li>✓ Implement security testing and assessment of app in this regard</li> </ul>	
Unmitigated risk score		Further mitigation controls required	
Likelihood	Possible	None	Likelihood
Impact	Extreme		Remote
Score	High Risk		Impact
			Score
			Very Low risk

### R 11. Risk: prolonged processing of data.

Risk	<b>Risk that the app continues processing data longer than justified.</b>		
Impact to the data subjects	Unfair processing and no-transparent processing leading to limitation of data subjects rights and freedoms.		
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ Follow the European Data Protection Guidelines for contact tracing apps (active only for the period of the COVID-19 crisis).</li> <li>✓ SLWG for the App holds the responsibility to trigger the orderly decommission of the app within 90 days of the COVID-19 crisis ending (declared by Scottish Ministers)</li> <li>✓ Introduce measures through the app and communications to prompt user action as appropriate as part of any wind-down</li> <li>✓ Continual review by the App SLGW for effectiveness</li> </ul>		
Unmitigated risk score		Further mitigation controls required	
Likelihood	Possible	None	Likelihood
Impact	Major		Remote
Score	Moderate Risk		Impact
			Score
			Very Low risk

### R 12. Risk: Anonymisation failure.

Risk	<b>Risk that personal identifiable data is not anonymised as expected</b>
------	---



Impact to the data subjects		Capturing and passing IP address and other identifiers from the device permit the data subject to be identified. This may limit the rights and freedoms of the data subjects and expose the individual to harm (e.g. financial loss, tracking, enforcement of isolation, etc.)			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ The app backend does not process IP addresses at the application layer. This means no IP address leaves the network layer on the backend.</li> <li>✓ All app backend logging does not log user IP address .</li> <li>✓ Open code for scrutiny.</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Remote
Impact	Major			Impact	Minor
Score	Moderate Risk			Score	Very Low risk

### R 13. Risk: Encryption failure.

Risk		<b>Risk that personal identifiable data in not encrypted as expected</b>			
Impact to the data subjects		Spam unencrypted SMS can identify the data subject. Restriction of data subjects rights and freedoms (e.g. tracking, privacy).			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Appropriate data processor agreements with SMS delivery service to protect confidentiality and thus protect data subjects</li> <li>✓ use known and trusted SMS provider for this service</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Likely	None		Likelihood	Remote
Impact	Moderate			Impact	Moderate
Score	Moderate Risk			Score	Very Low risk

### R 14. Risk: Ineffective app operation.

Risk		<b>Risk that technical issues with the app may compromise its effective operation.</b>			
Impact to the data subjects		Reduce user engagement and lessen its effectiveness in providing contact tracing.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Testing, including impact on other phone functions (e.g. battery life or interference with other Bluetooth peripherals)</li> <li>✓ Use Apple and Google ENS to benefit from their ability to optimise functioning of the exposure notification service beyond what any other app developer can</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Likely	None		Likelihood	Unlikely
Impact	Moderate			Impact	Minor
Score	Moderate Risk			Score	Very Low risk





### R 15. Risk: Bluetooth or ENS turned off.

Risk	<b>Risk that Bluetooth service is turned off beyond data subject awareness.</b>				
Impact to the data subjects	Turning off Bluetooth would disable the Contact Tracing function. The data subject may not receive exposure notifications when expected, and cause harm (exposure) to other people due to failure to self-isolate.				
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ Integrate into communications and within the app a clear message so people understand the impact of turning off Bluetooth on their phone</li> <li>✓ Clearly show, if people go into the app, that the Contact Tracing function is turned off</li> <li>✓ Ensure freedom of data subject (voluntary use, customization of settings) is not compromised</li> </ul>				
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	Reminder to switch Bluetooth back on feature in the app (next update of app)		Likelihood	Unlikely
Impact	Moderate			Impact	Moderate
Score	Moderate Risk			Score	Low risk

### R 16. Risk: Network / Mobile data.

Risk	<b>Risk that the app may use the App User network/mobile data allowance</b>				
Impact to the data subjects	This could incur additional costs for the user.				
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ Use a design that minimises the size of data downloads required. The amount of traffic sent to and from the device should not use up any significant portion of the user's monthly allowance or credit.</li> </ul>				
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Remote
Impact	Moderate			Impact	Minor
Score	Moderate Risk			Score	Very Low risk

### R 17. Risk: Discrimination

Risk	<b>Risk that the app may cause unlawful, unfair or unethical discrimination.</b>
Impact to the data subjects	<p>Digital exclusion. Unable to benefit from same health safeguards (test and protect measures) than other people.</p> <p>Anyone aged 15 and younger may feel Digitally excluded as they are below the age threshold to use the App.</p> <p>It is recognised that the depth of digital exclusion for people with disabilities is generally much greater than for the wider population. This disparity may include difficulties around access to the internet, lower digital skills and support. The Protect Scotland app has undergone accessibility through testing and improvements have been made.</p>





Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Refer to EQIA assessment available from <a href="https://protect.scot/">https://protect.scot/</a> (transparency section)</li> <li>✓ The Protect Scotland App does not create unlawful discrimination</li> <li>✓ The public engagement and marketing activity should help to identify any areas where the App may have disproportionate effects on people young or old.</li> <li>✓ The Scottish Government will work with DeafScotland, Disability Equality Scotland and Scottish Commission for Learning Disability (SCLD) to explore and address common barriers for people, with a disability and or a communication need in accessing the live Protect Scotland App.</li> <li>✓ The EQIA session captured the agreed mitigating actions which includes continued working with the equality organisations to ensure improved accessibility of information, processes are tested and the principles of inclusive communications are adopted.</li> <li>✓ The new Equalities &amp; Digital Inclusion Group will work with Digital Health &amp; Care to take this forward and in particular understand barriers to using the App.</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Likely	None		Likelihood	Likely
Impact	Moderate			Impact	Minor
Score	Moderate Risk			Score	Moderate risk

### R 18. Risk: Identity theft or fraudulent use of personal data

Risk		<b>Risk that personal data can be used to cause harm to the data subject as a result of identity theft or other fraudulent use of personal data.</b>			
Impact to the data subjects		Financial loss. Adverse consequences for the data subject (e.g. if used for fraudulent activities) that may include damaged credit, tax debt and criminal record.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Only minimum personal data with potential use on identity theft and fraud is used (mobile number).</li> <li>✓ Mobile numbers and SMS data is encrypted, is not stored beyond the minimum period required to send the SMS text messages and is anonymized (IP Address removed) at first opportunity.</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Unlikely
Impact	Moderate			Impact	Minor
Score	Moderate Risk			Score	Very Low Risk

### R 19. Risk: damage to reputation of the data subject

Risk		<b>Risk that personal data can be used to damage the reputation of the data subject</b>			
Impact to the data subjects		Damage to reputation with adverse consequences to the person within their family, friends or work environment.			



Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Only the minimum possible data is used, is anonymized at first opportunity, is not stored and is encrypted.</li> <li>✓ Location and tracking functionality is not engaged in the app</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Unlikely
Impact	Moderate			Impact	Minor
Score	Moderate Risk			Score	Very Low Risk

## R 20. Risk: automated processing.

Risk		<b>Risk of unconsented automated decisions.</b>			
Impact to the data subjects		Harm or adverse consequences due to recording Random IDs (close contacts) or sending exposure notifications without consent, inaccurate or without the opportunity to contest.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Terms and Conditions and privacy notice explain clearly what automated processing takes place in the app</li> <li>✓ Use of the app is voluntary</li> <li>✓ Download and installation requires explicit consent for automated processing purposes</li> <li>✓ Right to withdraw consent is embedded in the app (Leave function)</li> <li>✓ Right to contest automated decisions and how to exercise this right is explained in the privacy notice (helpline).</li> <li>✓ Accessible information, inclusive communication and marketing materials, including easy read (people with learning disabilities and literacy issues), languages other than English and bespoke to groups as required.</li> <li>✓ Continue to engage with stakeholders in Scotland and beyond on the impacts and challenges the App may present to different parts of the community.</li> <li>✓ Opportunity for users to feedback on the app on issues such as accessibility &amp; privacy</li> </ul>			
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible	None		Likelihood	Remote
Impact	Moderate			Impact	Negligible
Score	Moderate Risk			Score	Very Low Risk

## R 21. Risk: children and young people under 16 using the app

Risk		<b>Risk of children and young people under 16 using the app</b>			
Impact to the data subjects		No specific harm or adverse consequences to children or young adults have been identified. Some children may feel some concern or anxiety if they receive an Exposure Notification and have no adults to discuss the situation with.			
Privacy by design and by default notes.		<ul style="list-style-type: none"> <li>✓ Terms and Conditions, privacy notice, FAQs and marketing materials are clear on the legal age for downloading the app</li> <li>✓ On-boarding process requires explicit confirmation of age to allow download</li> </ul>			



		<ul style="list-style-type: none"> <li>✓ Use of the app is voluntary</li> <li>✓ Leave functionality is easy to use</li> <li>✓ Continue to engage with stakeholders in Scotland and beyond on the impacts and challenges the App may present to different parts of the community.</li> <li>✓ Opportunity for users to feedback on the app on issues such as accessibility &amp; privacy</li> <li>✓ Authorisation codes are not sent to people under 16; therefore children's Diagnosis Keys cannot be uploaded</li> <li>✓ Parental/carer responsibilities and guidance</li> <li>✓ Full Children rights and wellbeing assessment being undertaken to inform further measures and functionality of the app</li> </ul>		
Unmitigated risk score		Further mitigation controls required	Residual risk score	
Likelihood	Possible	Add further FAQs about parental guidance	Likelihood	Possible
Impact	Minor		Impact	Negligible
Score	Low Risk		Score	Very Low Risk

## R 22. Risk: people with specific disabilities using the app

Risk	<b>Risk of people with specific disabilities using the app</b>				
Impact to the data subjects	No specific harm or adverse consequences to this vulnerable group have been identified. Same impacts as described for other groups of the population within the specific risks discussed above. Potential higher impact for specific groups (e.g. PMLD).				
Privacy by design and by default notes.	<ul style="list-style-type: none"> <li>✓ Full Equality Impact Assessment undertaken to inform decisions about the app.</li> <li>✓ Helpline.</li> <li>✓ Accessible app, communications, resources and marketing materials.</li> <li>✓ App tested for accessibility. Further work with developers to improve accessibility.</li> <li>✓ App has no audio but is compatible with Google and Apple screen readers (settings on the data subject mobile phone).</li> <li>✓ The App can be used by any person in assistive, medical, care or similar capacity on behalf of another person.</li> <li>✓ The Equalities and Digital inclusion group work with vulnerable groups to understand accessibility and usability barriers. Opportunity for users to feedback on the app on issues such as accessibility &amp; privacy</li> <li>✓ Operation of the app is independent of the phone number (some vulnerable groups tend to change phone numbers more frequently).</li> <li>✓ PAMIS committed to working with their community and Scottish Government to further understand any issues and challenges around the App. It was acknowledged that if PMLD users were supported to download and set up the app, it would sit in the background.</li> </ul>				
Unmitigated risk score		Further mitigation controls required		Residual risk score	
Likelihood	Possible			Likelihood	Possible
Impact	Moderate			Impact	Minor
Score	Low Risk			Score	Low Risk

## 9 Necessity and Proportionality Assessment

This section, presents a reflective assessment of the necessity of the app and proportionality of the processing described in previous sections, including the measures taken comply with data subject rights, and data protections principles, but also to mitigated any identified risks to the rights and freedoms of people.

**Necessity of processing** requires that the proposed measures to be introduced will be effective for the objective pursued and whether it is less intrusive compared to other options for achieving the same goal.

On the other hand, the **proportionality of processing** requires that the advantages of the processing proposed are not outweighed by the disadvantages the measures may cause to a person's rights, and as such, a balance must be struck between the means used and the intended aim.

### **Necessity and Contact Tracing.**

The need to operate a form of contact tracing during the COVID-19 pandemic is beyond doubt. The basic operating principle is that on diagnosing a person with the disease, the close contacts of that person are identified, generally through interviews, and appropriate measures are taken in respect of those persons so identified to control the spread of the disease. This is an effective intervention in the fight against COVID-19 and has been deployed worldwide. However, there are inherent challenges to manual contact tracing.

In a review of international literature it was found that manual forms of contact tracing are overly reliant on recall (Leong et al., 2009) and it is argued that, for a highly infectious disease with a long incubation period, capacity to recall decreases and the likelihood of the disease being spread beyond known and usual contacts increases (Hart et al., April 2020). Furthermore, manual contact tracing also requires substantial human resources in the form of contact tracers (Hart et al., April 2020). Emerging literature suggests that manual contact tracing procedures is too slow,



lacks efficiency, and occurs at too small a scale to contain Covid-19 (Ferretti et al., March 2020, Hinch et al., April 2020). Additional measures have been introduced in Northern Ireland, and other countries, to aid in the control of the virus, such as severely restricting persons' movements, working habits and general day to day activities.

More recent studies suggest that in a model in which 15% of the population participated, it was found that digital exposure notification systems could reduce infections and deaths by approximately 8% and 6%, effectively complementing traditional contact tracing (Abueg et al, August 2020)<sup>19</sup>.

Key indicators of effective contact tracing are completeness of close contact identification and speed of close contact identification and subsequent follow-up, with a view to quickly and significantly reduce the viral transmission potential. The objective of using a mobile app based contact tracing solution as a supplement to the existing manual contact tracing is to increase the completeness of close contacts identified, and increase the speed in which those close contacts are identified and given the appropriate guidance.

Recently published data from the ONS survey has demonstrated that up to 79% of those who have a positive test result, have no symptoms on the day of testing, and no idea that they are infected. This means that the majority of people who have COVID-19 have no idea that they have it. To stop the infection spreading it is essential that those who do have symptoms get a test, and that if they test positive, we can identify people they have been in close contact with (<2m distance and >15min duration) so that they can be notified to self-isolate and avoid spreading the virus. This should take place as early as possible because most of those who are infected won't know it, and are likely spreading infection unknowingly. Identifying

---

<sup>19</sup> Abueg et al. "Modeling the combined effect of digital exposure notification and non-pharmaceutical interventions on the COVID-19 epidemic in Washington state". August 2020. <https://doi.org/10.1101/2020.08.29.20184135>



close contacts and advising them to self-isolate as early as possible is an effective approach to infection control.

Independent SAGE<sup>20</sup> has advised that to be effective in slowing the spread of COVID-19, contact tracing should aim to identify 80% of close contacts. Manual contact tracing has been demonstrated to help reduce the spread of infection but relies on people knowing those that they have been in close contact with, for them to be contacted.

As we come out of general lockdown and we move towards more targeted models of lockdown, as well as wintertime, the number of people we are in close contact with will increase substantially; many of them will be people unknown to us.

Manual contact tracing cannot possibly reach people unknown to us, so manual contact tracing on its own cannot possibly deliver the results required; the 'Protect Scotland' smartphone app is critical in helping with this challenge as allows notification between unknown people; this can provide a significant intervention in breaking chains of infection, when used as a measure to augment the manual contact process. The automated notification feature provided by the App can significantly speed up the process of notification, compared to manual methods. This is an essential advantage when time is critical to succeeding in breaking chains of infection.

It is significant to note that the Scottish Government decision to introduce an app based on the Apple and Google's ENS service will constitute a clear advantage compared with the difficulties that other countries have experienced when introducing apps not based on ENS (this technology wasn't available then), and have had significant functional problems, namely not functioning, or severely hampered

---

<sup>20</sup> Independent SAGE is a group of scientists who are working together to provide independent scientific advice to the UK government and public on how to minimise deaths and support Britain's recovery from the COVID-19 crisis. <https://www.independentsage.org/independent-sage/>

functioning, on iPhones, issues with battery life, and interference problems with Bluetooth peripherals. Furthermore, these apps have generally been based on a 'centralised' approach, where the public health authority requires access to a significant amount of contact tracing data of positive and close contacts, for which there have been privacy concerns raised. Concerns over these factors may have hampered adoption. The app recently deployed in the Republic of Ireland and Northern Ireland, which uses the same core code and architecture, was based on a 'decentralised' model. The level of uptake has been significant and rapid, with approximately 30% of the population downloading and installing the app within two weeks of launch, indicating significant levels of public confidence.

The use of ENS is intended to solve the referenced issues regarding the necessary core functionality proposition of 'proximity detection'. Furthermore, it is based on the decentralised model, removing the need to share contact traces with a central authority.

Alternative approaches to meeting the objectives stated above included the use of a centralised model and GPS/location tracking. While specific benefits prevail over the proposed approach for Scotland (namely assistance in cluster identification), significant privacy concerns exist with these approaches; therefore, Scottish Government decided not to pursue this route.

It is also expected that as more countries adopt the ENS, a consolidation of improvements in product robustness and interoperability across borders will emerge; there is considerable momentum across the EU for this.

The Protect Scotland app will have interoperability between the Scottish, the Republic of Ireland and the Northern Ireland apps. This is a significant development, supporting cross-border travel, and reducing chains of transmission when travelling.

Governance safeguards to limit the scope and extent of interference with data protection and privacy rights are in place through the terms of reference of the 'Protect Scotland App Short Life Working Group' (App SLWG) (see APPENDIX B –





App Governance), ensuring data is processed in line with its purpose and principles, including the full wind-down of data processing when the COVID-19 crisis is over, and the ongoing monitoring of the effectiveness of the app and appropriate wind-down if it is not. Through the design and implementation of the Contact Tracing function, these rights are further protected by ensuring it is and continues to be, entirely voluntary; and that users activation of the ENS is an integral part of the consensual adoption of the App, as well as the uploading of their diagnosis keys.

Location services are never used to track the location of users, where instead Bluetooth is used to detect proximity without any location data, meeting its purpose in a data minimised way.

People have control of the of features of the App that matter to them, including the ability to switch on/off ENS or notifications, as well as to Leave and delete the app the data at any time for the processing of all Contact Tracing data. It can be deleted under the control of the data subject, independently and without the knowledge of the Scottish Government or the NHS Scotland.

There is no consequence to not using the app as the Scottish Government or the NHS Scotland cannot tell who has and who hasn't installed the app.

**Having taken into consideration the necessity set out above, and the limited interference with data subject rights, the processing proposed under the Contact Tracing function of the app is seen as necessary and proportionate.**

### **Necessity and proportionality of App metrics.**

The processing of app metric data is a supporting form of processing for the performance of the above functions and to monitor their effectiveness. It is also intended to give the public health teams insights into the functioning of the app, such as the number of exposure notifications per day, for use in health policy formulation and measurement. It does not collect nor share personally identifiable information.





App users receive information about the collection of the data during the download and installation of the app and can decide to remove the app from their phone at any time.

It is considered to have no interference with individuals' rights since no personal data is involved; therefore, it is seen as necessary and proportionate. The data collected is essential in proving efficacy, as required for regulatory approval and the continued availability of the app.

## 10 Document control

Title	Protect Scotland App
Date Published/ Issued	16/9/2020
Date Effective From	10/9/2020
Version/ Issue Number	1.0
Document Type	Data Protection Impact Assessment
Document Status	Approved
Author	E. Beratarbide, National IG Lead, Digital Health and Care Directorate
Owner	J. Cameron, Deputy Director, Digital Health and Care Directorate
Approvers	C. Lamb, Director of Digital Reform and Service Engagement, Digital Health and Care Directorate
Contact	DHCIG@gov.scot
File Name	DPIA Protect Scotland App


## Revision History

Version	Date	Summary of Changes
1.0	16/09/2020	First published version of the DPIA for the Protect Scotland App.



## 10.1 Approval - Signoff

- Data Protection Officers from the data controllers (Scottish Government, Public Health Scotland and NHS National Services Scotland) have been engaged in the information governance process, providing advice and monitoring its performance pursuant to GDPR Article 35.
- Consultation has been sustained with the Information Commissioner's Office on a weekly basis.
- The overall risk position of the processing with regards to the rights and freedoms of the data subjects is considered low.
- The overall risk position of the processing with regards to the data controllers organisational risk low except for the overall cyber risk which remains moderate, and the adverse publicity (reputational) risk, which remains high. In this context, it is expected high public and media interest, and questions may be routed to Parliament.
- Having taken into consideration the necessity set out in this document (see section 9 Necessity and Proportionality Assessment), and the limited interference with data subject rights, the processing proposed for the Protect Scotland App is seen as necessary and proportionate.
- No compliance or ethical issues remain outstanding at this point. This will continue to be monitored as the App evolves through the governance structure set up for the App.

Version	Date	Name and designation	Electronic signature
1.0	16/09/2020	C. Lamb Director of Digital Reform and Service Engagement, Digital Health and Care Directorate	



## 11 APPENDIX A – Citizen engagement – Privacy Notice questionnaire

Questionnaire used for user feedback on the privacy notice and privacy concerns.

1. Have you read the full privacy notice? If not, what made you stop?

**\*Please read the full privacy notice before answering the following questions.**

2. Which of the following points do you feel more informed about after reading the privacy notice?

- what organisations are involved and what their role is regarding the app
- what the contact details for data protection officer are
- what the purposes of the app is
- what data is used by the app
- whether health data is used or not
- how your personal data is obtained
- how your phone number is obtained
- how your IP Address is obtained
- why it is necessary to process your data in the ways described
- what the legal basis for this is
- where your data goes
- who has access to your data
- whether your data goes outside the UK
- for how long your data is held and when it is deleted
- what your rights are and how to exercise them in the app

what to do if you don't want the app anymore

how to lodge a complaint with the Information Commissioner's Office

the automated decisions made by the app and how to contest automated decisions (e.g. by calling to a helpline etc.)

3. Is there anything missing from the privacy notice that you would want to know about?

4. What did you think of the language used in the privacy notice?

Did it feel like language you use in everyday life or was it more technical than you're used to?

5. What parts were very difficult to understand?

6. Do you have any suggestions that can help us make the privacy notice easier to understand?

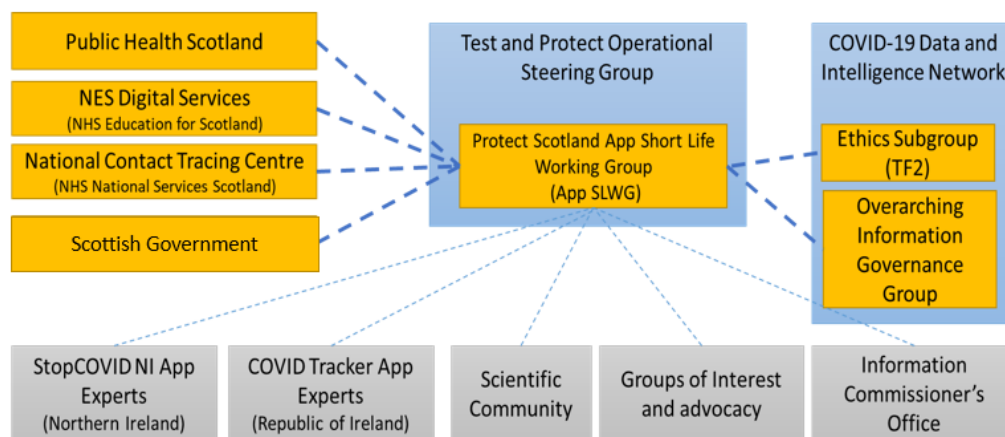


## 12 APPENDIX B – App Governance

### Governance approach

The Decision to proceed with the development of Protect Scotland was made by the First Minister and the Cabinet Secretary for Health & Sport. Delivery of the app was overseen a Short Life Working Group (SLWG), which was established as a sub-group of the Test & Protect Operational Steering Group. This followed an initial assessment by the Scottish Government’s Gold Command for Digital & Data. The SLWG had day to day governance responsibility for the development of the app, ensuring delivery and was a key decision maker. The SLWG comprised of senior policy, clinical and technical leads. Major go/no go decisions sat with Scottish Ministers, based on the advice from the SLWG.

AS Protect Scotland has been launched, the SLWG has completed its objective and a new Protect Scotland operational group will be setup under the Test & Protect Operational Steering Group to take forward future development and maintenance of the app. A robust change management process will also be established to ensure that all changes are considered and input is sought appropriately from clinical, technical, policy and information governance leads, and informed by public feedback. This group will also keep abreast of international developments related to proximity tracing technology.





### **PROTECT SCOTLAND APP SLWG Membership**

- (Chair) – Deputy Director, Test and Protect
- Deputy CMO
- Public Health Scotland (2)
- Head of Planning, NHS Lothian
- Deputy Head of Strategy and Insight, Marketing and Insight
- Deputy Director, Digital Health and Care
- Interim Head of Policy & Strategy, Digital Health and Care
- Head of Information Governance, Digital Health and Care
- Technical Lead
- User Design Lead
- Director, National Digital Service NHS NES
- Director of Digital and Security, NHS NSS

## 13 APPENDIX C – Digital and Data Ethics Summary

Scottish Government has judged our ability to demonstrate adherence to an ethical framework as essential in developing sufficient public trust to generate enough downloads across Scotland for the app to prove effective.

Ethical debates surrounding the use of digital health technologies have chiefly concerned the extent to which they provide anonymity for individuals, security for their personal information, and protection for their rights as members of a fair and lawful society.

Critical questions also concern the power and control different actors hold over these technologies and the data they yield. We know that the public's acceptance of passive digital health surveillance tools, their willingness to install and use mobile apps actively, and their comfort with different levels of data sharing, are influenced at least as much by their trust in these actors as in the technologies themselves.

The App SLWG have therefore considered, and agreed, an ethical framework guiding the development and use of the app. This is based on a published paper that identifies that Scotland's strategy for the public engagement should be guided by the emerging consensus on ethical considerations for COVID-19 apps.

The following questions are all considered as part of the Ethical Framework for all Covid-19 apps:

1. **The technology** – Will it work reliably? Is it safe? Is it secure? Is it private-by-design? Is it co-dependent on any other apps, databases or technologies (e.g., AI) that could alter these properties? Is the software code open to scrutiny by others?
2. **Its data privacy policies** – Does it capture or use only the minimum necessary data? Is consent required? How anonymous is it? Is it clear who it



will be shared with and for what purposes? Will it be deleted after COVID-19?  
Are these policies adequately explained and accessible to users?

3. **Its usefulness** – Is it really needed for this purpose? Does it achieve what it claims to? Is the value for citizens worth the privacy trade? Will it divert resources from more useful activities?
4. **Its optionality** – Are citizens free to choose whether or not to use the app, or particular features within it? If so, is this a genuine choice (e.g., not being able to return to work/ school otherwise)? Is it easy to control how data is shared by opting in or out?
5. **Its fairness** – Could be used in inequitable or discriminatory ways? Is it disproportionately intrusive, exploitative or coercive? Are the app and its benefits accessible to all (digital inclusion)? Could it restrict people's liberty?
6. **The people driving or developing it** – Are they being transparent about the project's ambitions and scope? Do they have secondary motives or conflicting interests?
7. **The institutions responsible for delivering it** – Is there sufficient oversight and accountability; are there adequate processes and expectations for stakeholder involvement?
8. **The users** – Is it vulnerable to misuse in ways that could harm or inconvenience others?

These ethical questions have been discussed with relevant groups of interests, including independent advocacy groups, such as Open Rights, the Scottish Privacy Forum, the NHS Scotland Public Benefit and Privacy Panel and the Information Commissioner's Office.

As a result, a "Digital and Data Summary" has been produced to illustrate the ethical rationale underpinning the adoption of the app as a measure to help with the COVID-19 pandemic. The latest version of this summary can be accessed from here: <https://protect.scot/> (Transparency section).



CORONAVIRUS 2019 (COVID-19)

# Protect-Scot App

More info [www link \(if available\)](#)

This App is part of a set of measures within the Scottish Government [Test and Protect Strategy](#).

Protect-Scot is a proximity tracing application based on Google/Apple coronavirus tracking API. Its function is to provide exposure notification to users who have been in contact (2 metres for 15 minutes) with other users that have received a positive COVID-19 test.

## DIGITAL AND DATA ETHICS

- ✓ Time limitation
- ✓ Testing and evaluation
- ✓ Proportionality
- ✓ Data minimization
- ✓ Use restriction
- ✓ Voluntariness
- ✓ Transparency
- ✓ Privacy
- ✓ Security
- ✓ Retention
- ✓ Infection reporting, notifications and no further tracking
- ✓ Accuracy
- ✓ Accountability
- ✓ Independent oversight
- ✓ Public engagement

## Scope

4.5 million

Adults in Scotland  
(+16 years)



## Benefits

- This App is an integral tool to support contact tracing processes in Scotland, helping to suppress the spread of the virus and support the lifting of current restrictions.
- Gives people the opportunity to know if they have been exposed to COVID-19 in the last 14 days
- Gives advice on what to do next if people have been exposed to the virus
- Is anonymous
- No centralised personal data

## CONTACT INFO

Lead

Digital Health and Care Directorate

Scottish Government

EMAIL

DHCIG@gov.scot

## COMPLIANCE

- ✓ Medical Devices Regulations
  - ✓ Data Protection (UK)\*
  - ✓ Common Law Duty of Confidentiality
  - ✓ Human Rights\*
  - ✓ Children Rights and Wellbeing\*
  - ✓ Equality\*
  - ✓ Fairer Scotland Duty\*
  - ✓ WHO ethical guidance for COVID-19 contact tracing
  - ✓ The Health and Social Care (Scotland) Public Benefit and Privacy Panel
  - ✓ The Scottish Privacy Forum
  - ✓ The Open Rights Group
- (\* Assessment available online.)

## No harm

- Using the App doesn't cause any harm to the population. If you use the App and have tested positive for COVID-19, the App does not track your movements at any point in time.
- The your privacy is not compromised, nor the privacy of any individuals who may have been in close proximity with you.
- The app does not store personal data.

## Autonomy

- Use of the App is completely voluntary.
- The App will not ask you for personal data
- The 'App settings' allow deletion of the App and any data stored on the phone
- You choose if you want to allow 'COVID-19 Exposure Notification Services' on your phone,
- You choose if you want to let others know they may be exposed to COVID (if you tested positive).
- You choose if you want to receive notifications or not

## Fairness & lawfulness

- A range of assessments, including data protection, human rights etc. have been carried out.
- Relevant groups, including expert epidemiologists, the Public Benefit and Privacy Panel, the Scottish Privacy Forum and the Open Rights Groups and the Information Commissioner Office have been consulted.
- The ProtectScotland App is considered a proportionate, fair and lawful measure.

## Transparency

- Collects anonymous stats for compliance with the Medicines and Healthcare Products Regulatory Agency.
- Your mobile number
- Your IP Address
- Scottish Government has no access to data other than some statistics used for planning the response to COVID along with Public Health Scotland.
- Consultation with key privacy and open rights groups, and the Information Commissioner Office.
- Full privacy notice and all other assessments available [here](#).





## 14 PPENDIX D – Risk scoring system

The risk assessments in this document are based on the NHS Scotland guidelines. Further information is available in [The Scottish Information Sharing Toolkit<sup>21</sup>](#).

---

<sup>21</sup> <https://www.informationgovernance.scot.nhs.uk/istresources/>



## Consequence / impact Table

Descriptor	Negligible	Minor	Moderate	Major	Extreme
<b>Objectives / Project</b>	Barely noticeable reduction in scope / quality / schedule of an eHealth innovation (e.g. new system)	Minor reduction in scope / quality / schedule	Reduction in scope or quality, project objectives or schedule	Significant project over-run	Inability to meet project objectives, reputation of the organisation seriously damaged (e.g. Care Data)
<b>Injury (Physical and psychological) to patient / visitor / staff.</b>  e.g. issues with data quality, availability or confidentiality with physical or psychological consequence for the data subject.	Adverse event leading to minor injury not requiring first aid  (e.g. data quality issues on instruction to patient re prescription)	Minor injury or illness, first aid treatment required	Agency reportable, e.g. Police (violent and aggressive acts) Significant injury requiring medical treatment and/or counselling.  e.g. Staff member who attempted suicide, privacy compromised as A&E shared details beyond "need-to-know".	Major injuries/long term incapacity or disability (loss of limb) requiring medical treatment and/or counselling.	Incident leading to death or major permanent incapacity  (e.g. health records not released on time for making treatment decision causing death or major injury).
<b>Patient Experience</b>  e.g. poor access to my records or difficulties to exert data protection rights.	Reduced quality of patient experience / clinical outcome not directly related to delivery of clinical care	Unsatisfactory patient experience / clinical outcome directly related to care provision – readily resolvable	Unsatisfactory patient experience / clinical outcome, short term effects – expect recovery <1wk	Unsatisfactory patient experience / clinical outcome, long term effects – expect recovery - >1wk	Unsatisfactory patient experience / clinical outcome, continued ongoing long term effects
<b>Complaints / Claims</b> e.g. Complaints due to data protection issues	Locally resolved verbal complaint	Justified written complaint peripheral to clinical care	Below excess claim. Justified complaint involving lack of appropriate care	Claim above excess level. Multiple justified complaints	Multiple claims or single major claim
<b>Service / Business Interruption</b>  e.g. from constant small interruptions of ICT systems to big Business Continuity issues due to cyberattacks or core data centre being down beyond acceptable levels.	Interruption in a service which does not impact on the delivery of patient care or the ability to continue to provide service	Short term disruption to service with minor impact on patient care	Some disruption in service with unacceptable impact on patient care Temporary loss of ability to provide service	Sustained loss of service which has serious impact on delivery of patient care resulting in major contingency plans being invoked.	Permanent loss of core service or facility Disruption to facility leading to significant "knock on" effect



Descriptor	Negligible	Minor	Moderate	Major	Extreme
<b>Staffing and Competence</b>  e.g. Poor data protection, confidentiality and ICT security training	Short term low staffing level temporarily reduces service quality (less than 1 day)  Short term low staffing level (>1 day), where there is no disruption to patient care	Ongoing low staffing level reduces service quality  Minor error due to ineffective training / implementation of training	Late delivery of key objective / service due to lack of staff. Moderate error due to ineffective training / implementation of training  Ongoing problems with staffing levels	Uncertain delivery of key objective / service due to lack of staff.  Major error due to ineffective training / implementation of training	Non-delivery of key objective / service due to lack of staff. Loss of key staff. Critical error due to ineffective training / implementation of training
<b>Financial (including damage / loss / fraud)</b>  e.g. derived from compensation rights as per DRA, ICO or NIS fines, ransomware, etc.	Negligible organisational / personal financial loss (£<10k)	Minor organisational / personal financial loss (£10k-100k)	Significant organisational / personal financial loss (£100k-250k)	Major organisational / personal financial loss (£250 k-1m)	Severe organisational personal financial loss (£>1m)
<b>Inspection / Audit</b>  e.g. ICO or NIS interventions	Small number of recommendations which focus on minor quality improvement issues	Recommendations made which can be addressed by low level of management action.	Challenging recommendations that can be addressed with appropriate action plan.	Enforcement action.  Low rating  Critical report.	Prosecution.  Zero rating  Severely critical report.
<b>Adverse Publicity / Reputation</b>  e.g. media attentions due to data breaches or cybersecurity attacks	Rumours, no media coverage  Little effect on staff morale	Local media coverage – short term. Some public embarrassment. Minor effect on staff morale / public attitudes.	Local media – long-term adverse publicity.  Significant effect on staff morale and public perception of the organisation	National media / adverse publicity, less than 3 days.  Public confidence in the organisation undermined Use of services affected	National / International media / adverse publicity, more than 3 days. MSP / MP concern (Questions in Parliament). Court Enforcement Public Enquiry
<b>Privacy</b>	Negligible harm to the individual arising from disclosure of confidential or sensitive information.	Minor harm to the individual arising from disclosure of confidential or sensitive information.  Uncomfortable situation with no material detrimental effect on the person.  Minor impact on dignity.	Moderate harm to the individual arising from disclosure of confidential or sensitive information  e.g. damage to personal relationships and social standing arising from disclosure of confidential or sensitive information	Major harm to the individual arising from disclosure of confidential or sensitive information  e.g. ID theft with potential adverse effect to the individual for which the person is likely to recover overtime or significant loss of personal autonomy  detrimental impact on dignity	Extreme harm to the individual arising from disclosure of confidential or sensitive information  e.g. ID theft with financial loss extreme adverse effect or  losing a job or  Extreme risk to life or health



### Likelihood of Recurrence definitions

Descriptor	Remote	Unlikely	Possible	Likely	Almost Certain
<b>Likelihood</b>	Can't believe this event would happen – will only happen in exceptional circumstances (5-10 years)	Not expected to happen, but definite potential exists – unlikely to occur (2-5 years)	May occur occasionally, has happened before on occasions – reasonable chance of occurring (annually)	Strong possibility that this could occur – likely to occur (quarterly)	This is expected to occur frequently / in most circumstances – more likely to occur than not (daily / weekly / monthly)

### Risk Assessment Matrix

Likelihood	Consequence				
	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Extreme (5)
<b>Almost certain (5)</b>	LR (5)	MR (10)	HR (15)	HR (20)	HR (25)
<b>Likely (4)</b>	LR (4)	MR (8)	MR (12)	HR (16)	HR (20)
<b>Possible (3)</b>	VLR (3)	LR (6)	MR (9)	MR (12)	HR (15)
<b>Unlikely (2)</b>	VLR (2)	LR (4)	LR (6)	MR (8)	MR (10)
<b>Remote (1)</b>	VLR (1)	VLR (2)	VLR (3)	LR (4)	LR (5)

- Very Low Risk (VLR)
- Low Risk (LR)
- Moderate Risk (MR)
- High Risk (HR)



## 15 Glossary, abbreviations and endnotes

### **App server**

The app server holds the anonymous diagnosis keys used by the app to allow those to be checked for a match with random IDs on other app users' devices. The app server also collects metric data.

### **Authorisation code or test result code**

A random code entered into the app by an app user who has had a positive COVID-19 test result, to allow exposure notifications to be provided to other app users.

### **CMS**

The National Contact Tracing Centre Case Management System provided by NHS NSS.

**CE marking** is a certification mark that indicates conformity with health, safety, and environmental protection standards for products sold within the European Economic Area.

### **Controller**

Any body which, alone or jointly with others, determines the purposes and means of the processing of personal information. Scottish Government, Public Health Scotland and NHS National Services Scotland are controllers in respect of personal information in connection with the app.

### **Diagnosis keys**



Random IDs sent from a user's device to the app server after that user has inserted an authorisation code on their app. We have explained here when diagnosis keys are considered personal information and when they are anonymised.

### **Exposure notification**

A notification provided by the app to an app user who has been in contact with an unnamed person who has tested positive for COVID-19, where the contact was recent enough, and for a sufficient time at a close enough distance, to mean that the app user receiving the notification may have been at risk of contracting the virus.

The notification does not include who the contact was with and where it was but does indicate date of potential infection.

### **IP address**

A numerical label assigned to a mobile device by the mobile phone or Wi-Fi service provider. It is typically made up of 4 sets of numbers (e.g. 192.168.0.50). As a consequence of how data traffic passes across the internet, the IP address is inevitably transferred to the app server.

### **National Contact Tracing Centre**

A service hosted within NHS NSS which will support the contact tracing function.

### **Personal information**

Any information relating to an identified or identifiable individual who can be identified, directly or indirectly from that information.

### **Processor**

Any body which processes personal information on behalf of the controller.



## Processing

Any action or operation which is performed on personal information (whether or not by automated means) such as collection, recording, storage, use, disclosure and destruction of personal information.

**Random IDs** (also known as identifier beacons, keys, anonymous rolling identifiers and Bluetooth IDs)

These are random numbers used by the app to create exposure notifications on app users' devices. You can learn more [here](#).