Privacy by design and default

As described in the section above, the app has been built to respect the ICO's Contact Tracing Principles. Key privacy features of the app are that:

- users' identities will not be revealed by the app
- no persistent user identifiers will be processed
- the app will collect the minimal amount of data necessary
- as far as possible processing will take place on user's phone
- personal data does not leave the device without the permission of the user
- self-declarations of relevant statuses are not verified with any external data source or process
- analytics data is only collected in anonymous form
- a performance view (via dashboards) using only aggregate and anonymous data to provide an oversight of the services provided by the NHS COVID-19 App
- there will be no third-party trackers gathering personal data in the app
- the user can delete the app and its data from their phone at any time
- data in the DHSC secure computing infrastructure will be made available only to individuals that have been formally authorised to access it
- transfer of data from the DHSC secure computing infrastructure to another system or controller, or processing for purposes outside the scope of this DPIA will be subject to further DPIA

The app makes use of the Google/Apple GAEN, which is incorporated in the operating systems of Apple and Android phones. The features which ensure user privacy are outlined in this document.

Contacts, QR codes, local authority and postcode district data is processed on the device. Circuit breaker, diagnosis keys and anonymous data are processed off the phone.

The GAEN

The app is built upon the contact matching functionality of the Google/Apple GAEN. The GAEN is subject to routine review and improvement by Google and Apple based upon the