Department of Health & Social Care

UMBRELLA MEMORANDUM OF UNDERSTANDING (UMoU)

BETWEEN

DEPARTMENT OF HEALTH AND SOCIAL CARE

AND

NATIONAL POLICE CHIEFS' COUNCIL

Acting on behalf of each of the police forces listed at Annex E to this UMoU in respect of the exchange of information for the self-isolation enforcement process

Published 22 March 2021

Contents

1. Participants to the UMoU

1) THE SECRETARY OF STATE FOR THE DEPARTMENT OF HEALTH AND SOCIAL CARE of 39 Victoria Street, London, SW1H 0EU hereafter referred to as **DHSC[1]"** throughout this document.

2) NATIONAL POLICE CHIEFS' COUNCIL (NPCC), of 1st Floor, 10 Victoria Street, London SW1H 0NN referred to as "**NPCC**" throughout this document, who is duly authorised to act on behalf each of the **"POLICE FORCES"** on a several basis as further listed at Annex E to the UMoU.

1.1 Collectively DHSC and the Police Forces are referred to as "Participants", and individually are referred to as a "Participant."

1.2 The NPCC is established pursuant to a collaboration agreement made pursuant to Section 22A of the Police Act 1996. That collaboration agreement provides pursuant to paragraph 7.1.3 a power for NPCC to co-ordinate the national police response to national emergencies. In this role, the NPCC represents that it is duly authorised to enter into this UMoU on behalf of each Police Force (on a several basis) relating to the information sharing arrangements between DHSC (as a Controller of Personal Data) and each Police Force (as a Controller of Personal Data as further identified in any process level MOU (PMoU)).

2. Introduction

2.1 This UMoU sets out the high-level information sharing arrangement between DHSC and the Police Forces that governs the exchange of information between the Participants. For the context of this UMoU "information" is defined as a collective set of data[2] and/or facts that when shared between the Participants through this UMoU or any associated purpose-specific information sharing MoUs can support the Participants to better deliver their respective business objectives and/or functions.

2.2. The aim of the UMoU is to set clear guidelines to follow when sharing information and to ensure that information is shared with appropriate safeguards and in accordance with the law.

Process Level MoUs

2.3 In addition to the UMoU, DHSC and Police Forces (acting, as the case may be through the NPCC) will approve and sign any specific Process level MoUs (PMoUs)

[1] DHSC – for the purpose of this UMoU refers to the DHSC as a 'competent authority' under The Data Protection Act 2018.

[2] All references to Data include Personal Data, Special Category Data, Non Personal Information, and de-personalised Information.
"Personal data" as meaning "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online.

for each purpose-specific information sharing activity between the Participants. The PMoUs will incorporate the terms of the UMoU and will include the information as set out in Annex B of this document. The PMoUs will be in the form set out in the "Process Level Template" attached to this UMoU. Each PMoU will reference the UMoU as the basis of exchange and must be read in conjunction with the UMoU.

Role of DHSC

2.4 All references to the DHSC in this document refer to DHSC as defined in Section 1 above.

2.5 This is a link to the DHSC website, which provides more information on the role of DHSC:https://www.gov.uk/government/organisations/department-of-health-and-social-care

Role of external organisations

2.6

- All references to the NPCC in this document refer to the NPCC, a non-statutory entity that is defined in Section 1 above and as further established pursuant to a Section 22A collaboration agreement made between the Police Forces (amongst others) to co-ordinate the work of the police service in order to protect the public.

- All references to a Police Force in this document refer to the Police Forces as further outlined at Annex E to this document.

- This is a link to the NPCC website that provides more information about the role of the NPCC: https://www.npcc.police.uk/. The NPCC website also provides further details in relation to the Police Forces.

2.7 A glossary of terms, abbreviations and definitions is provided at Annex C which equally applies to both the UMoU and PMoU.

3. Formalities

Date UMoU comes into effect

3.1 This UMoU came into effect on 14th October 2020 and was reviewed for an extended period between January and March 2021. See Annex D for details.

3.2 Amendments were identified as a result of the review and this version of the UMoU came into effect on 19th March 2021. See Annex D for details.

Date of review

3.3 This UMoU will be reviewed on 16th April 2021 and every 28 days thereafter.

4. Aims and objectives of UMoU.

4.1 Organisations which share data, particularly personal data, have a legal responsibility to ensure that the sharing is both lawful and subject to adequate controls.

4.2 This UMoU aims to:

- set out the high-level principles that will govern the sharing of information between the Participants including the onward disclosure of personal data to third parties (see section 17);
- describe the processes, structures and roles that will support the exchange of information between DHSC and the Police Forces;
- set out the legal responsibilities which apply to disclosure and use of personal data having regard to the Data Protection legislation[3];
- describe the data security procedures necessary to ensure compliance with the Data Protection legislation and any other specific security requirements;
- describe the process for managing personal data breaches; and
- describe the process for monitoring and reviewing the use of this UMoU.

5. Legal considerations to share information between the Participants.

5.1 Information will only be exchanged in a way which is compliant with the overarching principles of the Data Protection legislation (the UK GDPR[4] and Data Protection Act 2018), any statutory data sharing powers and where relevant the Common Law Duty of Confidentiality.

Powers to share information

5.2 Each PMoU will identify the specific statutory powers relied upon for each individual Participant for disclosing, receiving and/or further processing the information.

Lawful basis for processing personal data

5.3 In accordance with Articles 6, 9 and 10 of the UK GDPR and Section 35 of the Data Protection Act 2018, each PMoU will identify the lawful basis for disclosing, receiving and/or further processing the information for each Participant. Please see link to ICO Website for information on the Lawful Basis for processing personal data: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

[3] In this MoU, "Data Protection Legislation" has the same meaning as in section 3 of the Data Protection Act 2018

[4] UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4)

6. Privacy Information Notices

6.1 The Participants will ensure that their respective Privacy Information Notices (PINs) are sufficiently detailed to cover the information sharing activity specified in the respective PMoUs, including the purpose of the processing and the lawful basis for the processing.

7. Third Party Processing

7.1 (Where applicable) Each PMoU will identify any instances of third-party processing of personal data exchanged as a direct result of this UMoU or any associated PMoUs by either Participant. Where third parties are used, the relevant Participant will confirm that there are arrangements in place to ensure that the third party is compliant with the Data Protection legislation.

8. Data Protection Impact Assessments

8.1 The Participants will ensure that before any information sharing takes place under this UMoU, consideration is given as to whether a Data Protection Impact Assessment (DPIA) should be carried out. A DPIA will identify the relevant legal powers, lawful basis for the processing and assess the benefits of the information sharing, as well as identifying any privacy risks and how they might be mitigated. The DPIA is mandatory for DHSC.

9. Controller Status in respect of the Information Sharing

9.1 Each PMoU will identify the Controller status of the receiving Participant(s) in respect of the information sharing i.e. whether the receiving Participants (s) is/are a joint or sole controller of the data received.

10. General Principles

10.1 When completing and implementing the PMoUs, regard must be had to the following:

- the Participants will cooperate in good faith to fulfil the purposes of this UMoU and any PMoUs made under it;
- the Participants will make reasonable endeavours to ensure that the information being shared is checked before disclosure for accuracy and relevance. The disclosing Participant will ensure data integrity and that information sharing meets their standards. In the event that a Participant becomes aware of any inaccuracy or other defect in the information which has been disclosed it will notify the Participants which disclosed it;
- where anonymised information, pseudonymised information or non-personal information is shared, the recipient of that information will not attempt to re-identify any individual by analysing or combining it with other information which is in its possession at the time of receipt or subsequently comes into its possession;

- the Participants confirm that they have the technical capability and procedures in place to sufficiently comply with all the relevant data subject's rights under the Data Protection legislation including the technical capability to identify, provide and erase personal data should either Participant be legally required to do so; and,
- any personal data shared under this UMoU and any associated PMoUs must be proportionate, necessary and appropriate for the legitimate aim pursued.

11. Freedom of Information Act (FoIA) Requests

11.1 The Participants will demonstrate a commitment to openness and transparency regarding information sharing activities under this UMoU and any associated PMoUs.

11.2 In the event that any FoI request relating to information sharing activities under this UMoU or any associated PMoUs is received, the Participants accept to consult with the other in line with the Code of Practice made under section 45 of FoIA.

11.3 The Participant that receives a FoIA request will be responsible for responding to that request. The Participant that receives the request must alert the other Participant of the request.

12. Subject Access Requests (SAR)

12.1 Individuals can request a copy of all the information that either Participant holds on them, by making a SAR. This may include information that was disclosed to that Participant under this UMoU or any associated PMoUs. Where this is the case, as a matter of good practice, the Participants will liaise with each other to endeavour to ensure that the release of the information to the individual will not prejudice any ongoing investigation/proceedings.

13. Handling of Personal Data and Personal Data Security

13.1. Participants will be deemed to be independent Controllers (as defined in the Data Protection legislation) and as such must ensure that information shared that involves the sharing of personal data is handled and processed in accordance with the Data Protection legislation. Additionally, the Participants must process the information being shared in compliance with the mandatory requirements set by Her Majesty's Government Security Policy Framework ("HMG SPF") guidance issued by the Cabinet Office when handling, transferring, storing, accessing or destroying information assets. HMG SPF guidance document can be accessed via the following link https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework.

13.2 Data that is shared under this UMoU and any associated PMoU may only be shared and subsequently used for the purposes of investigating whether an offence has been committed under the Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020 and, as appropriate, enforcing the requirements set out in those regulations.

13.3 The Participants will ensure effective measures are in place to protect information in their care and manage potential or actual incidents of loss of information. By way of example without limitation, such measures may include:

- information not being transferred or stored on any type of portable device unless absolutely necessary, and if so, it must be encrypted and password protected to an approved standard;
- taking steps to ensure that all relevant staff are adequately trained and are aware of their responsibilities under the Data Protection legislation and this UMoU;
- access to information received by the Participants pursuant to this UMoU must be restricted to employees on a legitimate need-to-know basis, and with security clearance at the appropriate level;
- mailboxes will be regularly cleared down to reduce the impact of a compromise of the mailbox;
- in cases where shared mailboxes are used, secure access controls must be put in place, and assurance that these controls are in place, along with a Single Point of Contact for the mailbox, must be shared with the other Participant pursuant to this UMoU;
- data will ONLY be sent to named and authorised accounts/individuals that are able to request data;
- the movement of data between mailboxes must be password protected, and details of the password must be provided separately to the communication in which the data is shared (for example by providing two emails, one containing the data and another containing the password to access that data);only those with appropriate Baseline Personnel Security Standard clearances will have access;
- requests for personal data and responses containing personal data should be double checked/peer reviewed by someone with suitable experience or knowledge within the organisation dealing with the request, to ensure accuracy and verify recipient email addresses; and
- the Participants will comply with the Government Security Classifications Policy (GSCP) where applicable: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf.

13.4 Data will be shared on the understanding that the identities of those people who have been notified to self-isolate have not been verified by DHSC. The information may therefore be unsuitable to be used as primary evidence without further verification.

14. Case-by-case or individual disclosures of Information

14.1 Case-by-case/individual disclosures of information are permitted under this UMoU and can take place between the Participants on a regular basis through existing routes as long as they comply with the relevant Data Protection legislation

and the principles detailed in this UMoU. These exchanges will not be subject to an additional PMoU as described in section 2.

15. Method of information sharing

15.1 Information will be exchanged between Participants in a secure approved format, as approved by all Participants.

15.2 Participants will ensure that all information they transmit to each other will be marked with the appropriate security classification in accordance with the GSCP.

15.3 The method of exchange will be in accordance with the standards and benchmarks relating to the security of that transfer and in accordance with any applicable provisions of the Data Protection legislation, Cabinet Office and other HMG guidance.

16. Retention and destruction schedule

16.1 Participants undertake to store information received pursuant to this UMoU securely with access restricted to authorised personnel.

16.2 Participants will have documented policies on the retention and destruction of shared information in accordance with the requirements of the Data Protection legislation and HMG Security Policy Framework. Where specific information sharing activities are entered into by the Participants, the retention period should be jointly decided and set out in the respective PMoU for that information sharing activity.

16.3 Where a PMoU has been terminated, the Participants will follow any procedure set out in the PMoU in relation to the handling of information. If no specific provisions are decided, the Participants will co-operate to determine how the information shared between the Participants is handled.

16.4 Participants will retain and securely destroy shared information according to their own internal retention/destruction programme/schedule in line with the Data Protection legislation and in accordance with HMG Security Policy Framework guidance.

17. Onward disclosure of information to third parties

17.1 Participants will respect the confidentiality of the information being shared and will not disclose to third parties unless required to do so by law, or with the explicit consent of the other Participant or as stipulated at section 17.3 where lawful to do so below.

17.2 Unless otherwise stipulated within this UMoU, any information shared as a result of this UMoU and any associated PMoUs, which then forms part of the permanent record of the receiving Participant(s), becomes the responsibility of the receiving Participant(s) under the terms of the Data Protection legislation.

17.3 Participants accept that the information shared as a result of this UMoU and any associated PMoUs may also be used to update their respective internal records. As Controller for that data, the receiving Participant can disclose the information to third parties (this includes the sharing of information with external contractors or policing and criminal justice partners who are acting as Processors as on behalf of the Controller or a Controller in their own right) subject to the following conditions being met:

- the Participant making the onward disclosure must be satisfied that the information is only shared where it is necessary to carry out one of its own legitimate business functions and due regard must be had to any legal restrictions which may apply;
- the Participant making the onward disclosure must be satisfied that the information is being shared lawfully and in accordance with any legal obligations that may apply, including those set out in the Data Protection legislation;
- the Participant making the onward disclosure must be satisfied that adequate security arrangements are in place for the transmission of the data to the receiving Participant and that the receiving Participant has adequate security arrangements in place for the secure storage of the information, and
- where necessary a separate information sharing PMoU (or equivalent measures) should be put in place with the third-party organisation setting out all of the above.

18. Data subject complaint resolution procedure/Issues, disputes and resolution procedure between Participants

Data Subject Complaint Resolution Procedure

18.1 Complaints about the use of information in relation to this UMoU and any associated PMoUs should be dealt with under the relevant complaints procedure of the Participant whose actions are the subject of the complaint.

18.2 Participants agree to co-operate with each other in the investigation of any complaint or other investigation about the use of the information shared.

18.3 The outcome/resolution of any complaint will be notified to the other Participant to this UMoU.

Issues, Disputes and Resolution between Participants Procedure

18.4 Any issues or disputes that arise as a result of exchanges covered by this UMoU or associated PMoUs must be directed to the relevant contact points listed in Annex A or E as listed in the relevant PMoU. Each Participant will be responsible for escalating the issue as necessary within their given organisations.

18.5 Where an issue or dispute arises it should be reported as soon as possible. Should the problem be of an urgent nature, it must be reported by phone immediately to the designated business as usual contact (listed in Annex A or E, as

appropriate) and followed up in writing the same day. If the problem is not of an urgent nature it can be reported in writing within 24 hours of the problem occurring.

18.6 Any deviation from this process that is required by either DHSC, a Police Force, or the NPCC acting on behalf of each of the Police Forces in respect of a particular information sharing activity will be detailed in the relevant PMoU.

19. Monitoring and reviewing arrangements

19.1 The UMoU will run for 12 months but must be reviewed after 21 days of the UMoU coming into effect and every 28 days thereafter.

Review process

19.2 The review process will focus on:

- confirming whether the UMoU includes the correct contact details for key personnel;
- whether the UMoU is still necessary and fit for purpose;
- whether the existing information sharing arrangements should be extended or amended; and
- whether the legal bases relied upon by the Participants for sharing the information remain valid, including whether any legislation has been amended or enacted that would impact on any purpose-specific information sharing activities. If a Participant's legal basis for information sharing has changed, the information sharing activity in place may need to be amended to reflect this.

19.3 Any changes needed in the interim may be approved in writing and appended to this document for inclusion at the following review.

19.4 Reviews outside of the approved schedule can be called by representatives of DHSC, a Police Force or the NPCC (acting on behalf of each of the Police Forces), for example where new or revised legislation or cross-government guidance necessitates an earlier review.

19.5 A record of the review will be created and retained by DHSC and each of the Police Forces to the extent the Police Forces were a party to such review.

19.6 Annex D outlines the contacts for document control, the version history of this UMoU and the review dates for it.

Monitoring compliance

19.7 DHSC and each individual Police Force (acting, as the case may be, through the NPCC) reserves the right to carry out a review of compliance with the terms of this UMoU and any associated PMoUs and accept to co-operate fully with any such review.

20. Costs

20.1 Participants will pay their own costs and provide adequate resources to perform their activities under this UMoU. There may, however, be charges levied in specific information sharing exchanges in relation, for example, to IT development. These will be detailed in the respective PMoU.

21. Termination

21.1 DHSC, a Police Force (as between itself and DHSC only) or the NPCC (acting on behalf of each of the Police Forces or in respect of the all of the Police Forces) (a Terminating Party) will have the right to terminate this UMoU by giving two weeks' notice of termination in writing to each other should the following circumstances arise:

- a material breach by the other Participant of any of the terms of the UMoU;
- by reason of cost, resources or other factors beyond the control of either of the Participants; and/or
- if any material change in circumstances occurs which, following negotiation between the Participants, in the reasonable opinion of either or all of the Participants significantly impairs the value of the UMoU in meeting their objectives.

21.2 In the event that a Police Force is the Terminating Party seeking to terminate this UMoU, any such termination shall only take effect as between that Police Force and DHSC. The UMoU shall survive as between the other Police Forces unless terminated by the other Police Forces or the NPCC acting on their behalf. Termination of the UMoU will have the effect of automatically making void all PMoUs made between the relevant terminating parities under the terms of the UMoU.

21.3 Where a PMoU has been terminated, DHSC and the Police Forces that are party to that PMoU will follow any procedure set out in the PMoU in relation to the handling of the information shared. If no specific provisions are decided, DHSC and the Police Forces will co-operate to determine how the information shared between the Participants is handled.

21.4 In the event of a significant personal data breach or other serious breach of the terms of this UMoU by any of the Participants, this UMoU must be reviewed immediately by DHSC and the Police Forces.

21.5 The Participants understand that the provisions of this UMoU will continue to apply to any information previously shared pursuant to this UMoU and any of its PMoUs, notwithstanding the termination of this UMoU.

22. Personal Data Breaches

22.1 A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorised disclosure of, or access to personal data transmitted stored or otherwise processed.

22.2 Examples of serious personal data breaches may include:

- accidental loss or damage to the personal data;
- damage or loss of personal data by means of malicious software/hacking;
- deliberate or knowing disclosure of personal data to a person not entitled to receive the data;
- emailing classified/sensitive information containing personal data to personal email accounts;
- leaving classified/sensitive papers containing personal data in an unsecure or publicly accessible area;
- using social networking sites to publish information containing personal data which may bring either Participant's organisations into disrepute.

22.3 The designated points of contact (provided at Annex A or E (as appropriate) of this UMoU) are responsible for notifying the other Participant in writing in the event of personal data breach within 24 hours of becoming aware of the event.

22.4 The designated points of contact will discuss and jointly decide the next steps relating to the incident, taking specialist advice where appropriate. Such arrangements will include (but will not be limited to) containment of the incident and mitigation of any ongoing risk, recovery of the personal data, and assessing whether the Information Commissioner and/or the data subjects will be notified. The arrangements may vary in each case, depending on the sensitivity of the personal data and the nature of the loss or unauthorised disclosure.

22.5 Where appropriate, and if relevant to the incident, disciplinary misconduct action and/or criminal proceedings may be considered.

23. Signatories

Signed on behalf of DHSC:

23.1 I accept the terms of the Memorandum of Understanding on behalf of DHSC.

Signature:	[redacted]
Name:	[redacted]
Date:	19 March 2021
Position:	Deputy Senior Information Risk Owner for the Department of Health and Social Care

Signature:	[redacted]
Name:	[redacted]
Date:	19 March 2021
Position:	Data Protection Officer for the Department of Health and Social Care

Signed on behalf of NPCC

23.2 I accept the terms of the Memorandum of Understanding on behalf of NPCC.

Signature:	[redacted]
Name:	[redacted]
Date:	19 March 2021
Position:	Chair of the NPCC on behalf of the each of the Police Forces

Annex A - Business Contacts

Business as Usual Contacts - DHSC

Contact	Email	Responsibility
DHSC	[redacted]	Complaints/Issues /Disputes and Resolution
DHSC Legal	[redacted]	Legal Issues
FOI	freedomofinformation@dhsc.gov.uk	Freedom of Information
Delivery Lead	[redacted]	Review and amendments to MoU
DHSC Data Protection Team	[redacted]	Personal Data Breaches

Business as Usual Contacts – NPCC

Contact	Email	Responsibility
NPCC	[redacted]	Complaints/Issues /Disputes and Resolution
NPCC Legal	[redacted]	Legal Issues
FOI	npcc.foi.request@cru.pnn.police.uk	Freedom of Information
NPCC	[redacted]	Review and amendments to MoU
NPCC	[redacted]	Personal Data Breaches

Escalation Contacts – DHSC

Contact	Email	Responsibility
DHSC	[redacted]	Complaints/Issues /Disputes and Resolution

DHSC Legal	[redacted]	Legal issues
FOI	Freedomofinformation@dhsc.gov.uk	Freedom of Information
Delivery Lead	[redacted]	Review and amendments to MoU
DHSC Data Protection Team	[redacted]	Personal Data Breaches

Escalation Contacts – NPCC

Contact	**Email**	**Responsibility**
Deputy Head of Unit – NPCC	[redacted]	Complaints/Issues /Disputes and Resolution
NPCC Legal	[redacted]	Legal
[redacted] Freedom of Information Officer & Decision Maker	npcc.foi.request@cru.pnn.police.uk	Freedom of Information
NPCC Legal	[redacted]	Review and amendments to MoU
[redacted] NPCC Data Protection Officer	[redacted]	Personal Data Breaches

Annex B - Information exchange specific (process-level) MoUs

As a minimum all PMoUs should include:

- the purpose of the exchange;
- the physical method of exchange;
- the benefit of the exchange;
- the method by which the information shared is to be handled and kept secure by the recipient;
- the legal powers relied upon for the specific PMoU;
- the lawful basis for processing personal data;
- the fiscal cost (if appropriate);
- confirm if a PIN is in place that sufficiently covers the information sharing activity;
- confirm if DPIA has been carried out;
- the roles and responsibilities of the Participants including (if appropriate) which Participant(s) will act as a Controller or Processer; and
- a formal review date.

Where onward disclosure is envisaged, the PMoU should put in place any arrangements necessary to ensure that this occurs in accordance with the Participants' legal obligations. The PMoU should also detail reporting arrangements for any security incidents that involve exported information after onward disclosure.

PMoU description	Legal Basis	Business Owner	Start Date

Annex C - Glossary of terms, abbreviations and definitions

In this MoU the following words and phrases will have the following meanings, unless expressly stated to the contrary:

Definition	Interpretation
Controller	Has the same meaning as defined in the Data Protection Legislation, that is, the person who determines the manner in which and purposes for which personal data are to be processed, either alone or jointly in common with other persons.
Processor	Has the same meaning as defined as Processor or Data Processor in the Data Protection Legislation, that is, any person who processes personal data on behalf of the Controller (other than an employee).
Data Protection Legislation	Has the same meanings as in section 3(9) of the Data Protection Act 2018
Guidance	(where applicable) The guidance and codes of practice issued by the Information Commissioner.
Law	Means any applicable law, statute, byelaw, regulation, and/or order.
Policy/rule of court etc	Regulatory policy, guidance or industry code, rule of court or directives or requirements of any Regulatory Body, delegated or subordinate legislation or notice of any Regulatory Body.
Participants	Means Participants to this MoU and refers explicitly to DHSC. References to any other Government Department will be explicitly referenced where required
Data Subject	Has the same meaning as defined in the Data Protection Legislation, being an identified or identifiable natural person who is the subject of personal data
Personal Data	Means any information relating to a data subject who can be identified from it or

	data that can be put together with other information to identify a living individual. It covers data held in any format.
Data Protection Impact Assessment (DPIA)	A tool that can be used to identify and reduce the privacy risks of any activity where personal data is processed (including information sharing).
United Kingdom General Data Protection Regulation (UK GDPR)	Means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (United Kingdom General Data Protection Regulation), as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (and see section 205(4))
Privacy Information Notice (PIN)	Means a publicly available statement or document that sets out some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfils a legal requirement to protect a customer or client's privacy.
Non–Personal Information	Information that has never referred to an individual and cannot be connected to an individual.
Information	Defined as a collective set of Data and/or facts that, when shared between the Participants through this UMoU or any associated purpose-specific data sharing MoUs, can support the Participants to better deliver their respective business objectives and/or functions. It includes personal data, special category data, non-personal information and de-personalised information.
Process/Processed/ Processing	Have the same meaning as defined in the Data Protection Legislation and includes collecting, recording, storing, retrieving, amending or altering,

	disclosing, deleting, archiving and destroying personal data.
Umbrella MoU (UMoU)	These documents are used when entering into an information sharing activity with another government department where the intention/ expectation is that there will be a regular or significant amount of information sharing taking place involving personal data. The UMoU sets out the overarching principles of information sharing between the Participants.
Process MoU (PMoU)	DHSC terminology. A process MoU is approved and signed by DHSC and each of the Police Forces for each category of data which will be shared or for each purpose-specific information sharing activity and is in the format set out in the PMoU Template attached to the UMoU.

Annex D Document Control

Document Control Personnel

Key personnel	Name	Organisation (Team)
Author	[redacted]	DHSC
Approver	[redacted] [redacted]	DHSC NPCC
Review Control	[redacted] [redacted]	DHSC NPCC

Version and review History

Version / review	Date	Summary of changes	Changes marked
V1	14/10/2020	UMoU agreed and signed	
V2	02/11/2020	Document formatted for consistency DHSC contacts added	
V3	19/03/2021	Updated to reflect amended regulations, legislative references and the police enforcement process.	

Annex E List of Police Forces

A list of Police Forces and their contact details are set out below in the event of any enquiries arising in respect of the data sharing under this UMoU.

Name of police force	Contact, correspondence address and email	Link to Privacy Information Notice
Avon and Somerset Constabulary	The Data Protection Officer Avon and Somerset Constabulary, Police & Fire Headquarters, PO Box 37, Valley Road, Portishead, Near Bristol, BS20 8QJ [redacted]	https://www.avonandsomerset.police.uk/help/privacy/privacy-notice/
Bedfordshire Police	[redacted] Head of Information Management Bedfordshire Police Headquarters Woburn Road Kempston Bedford MK43 9AX [redacted]	https://www.bedfordshire.police.uk/information-and-services/About-us/Privacy-notice/Privacy-intro
British Transport Police	Information Governance Unit 2nd Floor 3 Callaghan Square Cardiff CF10 5BT [redacted]	https://www.btp.police.uk/about_us/your_right_to_information/data_protection.aspx
Cambridgeshire Constabulary	[redacted] Head of Information Management Bedfordshire Police Headquarters Woburn Road Kempston	https://www.cambs.police.uk/information-and-services/About-us/Privacy-notice/Privacy-intro

	Bedford MK43 9AX [redacted]	
Cheshire Constabulary	Data Protection Officer Cheshire Constabulary HQ Clemonds Hey Oakmere Road Winsford Cheshire CW7 2UA [redacted]	https://www.cheshire.police.uk/hyg/fpncheshire/privacy-notice/
City of London Police	[redacted] Director of Information (CISO & DPO) [redacted]	https://www.cityoflondon.police.uk/hyg/city/privacy-notice/ https://www.cityoflondon.police.uk/hyg/cv/coronavirus-covid-19-privacy-notice/
Civil Nuclear Constabulary	Disclosures Officer Civil Nuclear Constabulary Culham Science Centre Abingdon Oxfordshire OX14 3DB [redacted]	https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about/personal-information-charter
Cleveland Police	[redacted] Data Protection Officer Cleveland Police Shared Service Centre Ash House III Acres Princeton Drive Thornaby Stockton on Tees TS17 6AJ [redacted]	https://www.cleveland.police.uk/hyg/fpscleveland/privacy-notice/
Cumbria Constabulary	Force Disclosure Manager/Data Protection Officer	https://www.cumbria.police.uk/About-this-site/Website-Privacy-Notice.aspx

	People Department, Corporate Support Cumbria Constabulary Police Headquarters Carleton Hall Penrith Cumbria CA10 2AU [redacted]	
Derbyshire Constabulary	Data Protection Team Derbyshire Constabulary Butterley Hall Ripley Derbyshire DE5 3RS [redacted]	https://www.derbyshire.police.uk/hyg/fpnderbyshire/privacy-notice/
Devon and Cornwall Police	Data Protection Officer Alliance Data Protection Office, Devon and Cornwall Police Police Headquarters Middlemoor, Exeter Devon EX2 7HQ [redacted]	https://www.devon-cornwall.police.uk/your-right-to-information/data-protection-requests/information-charter-privacy-notice-fair-processing/
Dorset Police	Data Protection Officer Alliance Data Protection Office, Devon and Cornwall Police Police Headquarters Middlemoor, Exeter Devon EX2 7HQ [redacted]	https://www.dorset.police.uk/news-information/legal-privacy/
Durham Constabulary	Data Protection Officer	https://www.durham.police.uk/About-Us/Freedom-of-information/General/Documents/

	[redacted]	Durham%20Constabulary%20Privacy%20Notice%20v5-0.pdf
Essex Police	[redacted] Data Protection Officer Essex Police HQ PO Box 2 Chelmsford CM2 6DA [redacted]	https://www.essex.police.uk/hyg/fpnessex/privacy-notice/
Gloucestershire Constabulary	[redacted] Data Protection Officer Information Disclosure Gloucestershire Constabulary Police HQ 1 Waterwells Drive Waterwells Quedgeley GL2 2AN	https://www.gloucestershire.police.uk/hyg/fpngloucs/privacy-notice/
Greater Manchester Police	The Data Protection Officer Information Compliance and Records Management Unit Greater Manchester Police Information Services Branch Openshaw Complex Lawton Street Manchester M11 2NS [redacted]	https://www.gmp.police.uk/hyg/fpngmp/privacy-notice/
Hampshire Constabulary	Data Protection Officer Mottisfont Court Tower Street Winchester Hampshire SO23 8ZD	https://www.hampshire.police.uk/hyg/fpnhc/privacy-notice/

	[redacted]	
Hertfordshire Constabulary	[redacted] Head of Information Management Bedfordshire Police Headquarters Woburn Road Kempston Bedford MK43 9AX [redacted]	https://www.herts.police.uk/Information-and-services/About-us/Privacy-notice/Privacy-notice
Humberside Police	[redacted] Data Protection Officer Humberside Police Information Compliance Police HQ Priory Road Hull HU5 5SF	https://www.humberside.police.uk/data-protection-privacy-notice
Kent Police	Data Protection Officer Information Security and Governance Department Kent Police Coldharbour London Road Aylesford ME20 7SL [redacted]	https://www.kent.police.uk/hyg/fpnkent/privacy-notice/
Lancashire Constabulary	Data Protection Officer Lancashire Constabulary Police Headquarters PO Box 77 Lancashire PR4 5SB [redacted]	https://www.lancashire.police.uk/information/privacy-notice/
Leicestershire Police	Data Protection Team Information Management Unit Police Headquarters	https://www.leics.police.uk/hyg/fpnleic/privacy-notice/

	St Johns Enderby Leicester LE19 2BX [redacted]	
Lincolnshire Police	Data Protection Officer Information Management Unit, Police Headquarters, PO Box 999, Lincoln, LN5 7PH [redacted]	https://www.lincs.police.uk/resource-library/data-protection/privacy-notice/
Merseyside Police	[redacted] Data Protection Officer Merseyside Police PO Box 59 Liverpool L69 1JD [redacted]	https://www.merseyside.police.uk/hyg/fpnmerseyside/privacy-notice/
Metropolitan Police Service	[redacted] Data Protection Officer c/o Information Rights Unit PO Box 313 Sidcup DA15 0HH [redacted]	https://www.met.police.uk/hyg/fpnm/privacy/
Ministry of Defence Police	Data Protection Office Room 23, Building 1071 MDP HQ Wethersfield Braintree Essex CM7 4AZ [redacted]	https://www.gov.uk/government/publications/ministry-of-defence-police-privacy-notice/ministry-of-defence-police-privacy-notice

Norfolk Constabulary	Data Protection Officer Norfolk Constabulary Operations and Communications Centre Jubilee House Falconers Chase Wymondham Norfolk NR18 0WW [redacted]	https://www.norfolk.police.uk/about-us/our-data/data-protection/privacy-notice-coronavirus-covid-19
North Yorkshire Police	[redacted] North Yorkshire Police Headquarter North Yorkshire Police Alverton Court Crosby Road Northallerton North Yorkshire DL6 1BF [redacted]	https://northyorkshire.police.uk/access-to-information/privacy-notice/
Northamptonshire Police	Information Unit Manager Force Headquarters Wootton Hall Wootton Hall Park Northampton NN4 0JQ [redacted]	https://www.northants.police.uk/hyg/fpnnorth/privacy-notice/
Northumbria Police	[redacted] Force Data Protection Officer Northumbria Police Schalksmuhle Road Bedlington Northumberland NE22 7LA [redacted]	https://beta.northumbria.police.uk/cookies-and-privacy/
Nottinghamshire Police	Data Protection Officer	https://www.nottinghamshire.police.uk/sites/default/files/documen

	Information Management Unit Headquarters Sherwood Lodge Arnold Nottingham NG5 8PP [redacted]	ts/files/NottsPrivacy_Notice_25.05.2018.pdf
South Yorkshire Police	Data Protection Officer [redacted]	https://southyorks.police.uk/media/5745/privacy-notice-covid-19.pdf
Staffordshire Police	The Data Protection Officer Staffordshire Police Headquarters Weston Road Staffordshire ST18 0YY [redacted]	https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/
Suffolk Constabulary	Data Protection Officer Suffolk Constabulary Police Headquarters Martlesham Heath Ipswich Suffolk IP5 3QS [redacted]	https://www.suffolk.police.uk/about-us/our-data/data-protection/privacy-notice-coronavirus-covid-19
Surrey Police	Data Protection Officer Surrey Police PO Box 101 Surrey Guildford GU1 9PE [redacted]	https://www.surrey.police.uk/hyg/fpnsurrey/privacy-notice/
Sussex Police	Data Protection Officer Sussex Police	https://www.sussex.police.uk/hyg/fpnsussex/privacy-notice/

	Headquarters Church Lane Lewes East Sussex BN7 2DZ [redacted]	
Thames Valley Police	Data Protection Officer Thames Valley Police Public Access Office Oxford Road Kidlington OX5 2NX [redacted]	https://www.thamesvalley.police.uk/hyg/fpntvp/privacy-notice/
Warwickshire Police	Data Protection Officer Warwickshire Police Audit, Risk and Compliance Department, PO Box 55 Hindlip Worcester WR3 8SP [redacted]	https://www.warwickshire.police.uk/hyg/fpnwarwickshire/privacy-notice/
West Mercia Police	Data Protection Officer West Mercia Police Audit, Risk and Compliance Department PO Box 55 Hindlip Worcester WR3 8SP [redacted]	https://www.westmercia.police.uk/hyg/fpnwestmercia/privacy-notice/
West Midlands Police	Information Security and Assurance West Midlands Police PO Box 52 Birmingham B4 6NQ	https://www.west-midlands.police.uk/about-us/privacy-notice

	[redacted]	
West Yorkshire Police	[redacted] Data Protection Officer PO BOX 9 Laburnum Road Wakefield WF1 3QP [redacted]	https://www.westyorkshire.police.uk/advice/our-services/your-data/privacy-information-notice/privacy-information-notice
Wiltshire Police	Data Protection Officer Wiltshire Police HQ London Road Devizes Wiltshire SN10 2DN [redacted]	https://www.wiltshire.police.uk/media/2289/Wiltshire-Police-privacy-notice/pdf/Wiltshire_Police_privacy_notice.pdf?m=636802203005570000

PROCESS LEVEL MEMORANDUM OF UNDERSTANDING (PMoU)

BETWEEN

NATIONAL POLICE CHIEFS' COUNCIL (NPCC)

Acting on behalf of each of the Police Forces listed at Annex C to this PMoU

AND

DEPARTMENT OF HEALTH AND SOCIAL CARE

Sharing of data to enable self-isolation enforcement process

Contents

1. Introduction and Participants to the PMoU

1.1 This is a PMoU made under the terms of the overarching UMoU between NPCC on behalf of each of the Police Forces listed at Annex C to this PMoU on a several basis, and DHSC. Any information shared pursuant to this PMoU is subject to the provisions set out in the UMoU between DHSC and NPCC (on behalf of each of the Police Forces) including any conditions set out therein and this PMoU should therefore be read in conjunction with the UMoU

1.2 This PMoU will be entered into by NPCC (on behalf of each of the Police Forces) and DHSC, who are responsible for the purpose-specific information sharing activity to which this PMoU relates.

1.3 Collectively DHSC and the Police Forces are referred to as 'Participants', and individually are referred to as a "Participant."

2. Formalities

Date PMoU comes into effect

2.1 This PMoU came into effect on 14th October 2020 and was reviewed for an extended period between January and March 2021. See Annex A for details.

2.2 Amendments were identified as a result of the review and this version of the PMoU came into effect on 19th March 2021. See Annex A for details.

Date of review

2.3 The date of the review of this PMoU is 16th April 2021 and every 28 days thereafter.

3. Powers to share personal data between the Participants

3.1 The relevant legal bases to share information involving personal data between the Participants are set out below.

DHSC

3.2 The Health Protection (Coronavirus, Restrictions) (Self-Isolation) (England) Regulations 2020 ("the Regulations") made under sections 45B, 45C(1) and (3)(c), 45D, 45F(2), 45P and 45T(6) of the Public Health (Control of Disease) Act 1984 impose restrictions on people who are notified (by the bodies specified in the regulations) they have tested positive for coronavirus or who are notified that they have been in close contact with a person who has tested positive, in order to prevent the spread of infection or contamination from coronavirus or coronavirus disease. A reference to the Regulations in the PMoU includes a reference to the Regulations as the same may be amended, restated or superseded from time to time.
Regulation 14 provides a statutory power for certain personal data collected under the Regulations to be used and disclosed for certain purposes, including for the

purposes of performing a function under the Regulations, where there might otherwise have been a duty of confidence or other restriction on disclosure. It is primarily under this power that DHSC will use personal data and disclose personal data to the Police Forces for the purposes of this PMoU to facilitate their law enforcement purposes under the Regulations. In addition, there are powers in section 2A of the National Health Service Act 2006 and section 115 of the Crime and Disorder Act 1998 pursuant to which information may be disclosed. Personal data will only be shared under this PMoU and subsequently used by a receiving party for the purposes set out in the Regulations, which is principally for enforcing the Regulations.

3.2.1 The sharing of personal data by DHSC with the Police Forces is considered a necessary and proportionate measure to achieve the substantial public interest of preventing danger to public health. This data sharing allows Police Forces to effectively enforce the Regulations.

The information provided will allow the police to deal with breaches of the Regulations brought to their attention or in the course of their duties whether by issuing fixed penalty notices or pursuing prosecutions in accordance with the powers entrusted to the Police Forces under the Regulations. The information provided is crucial in that it will ensure police officers can distinguish between the types of cases and related circumstances in order that they may effectively investigate and evidence each individual case. This information will allow Police Forces to risk assess and respond to situations effectively.

3.2.2 The data to be shared can be defined in three ways. ‘Relevant information’, ‘notification information’, and ‘contextual information’.

a) ‘Relevant information’, as set out in section 10.3, provides for sharing of details including name, date of birth, contact information (telephone number, email address, home/self-isolation address), and gender as well as information regarding their self-isolation (including date of notification to self-isolate and required period of self-isolation). ‘Relevant information’ may only be disclosed for the purposes of carrying out a function under these Regulations, such as to ensure compliance with the legal duty to self-isolate or to prevent danger to the health of the public as a result of the spread of infection or contamination of coronavirus.

This information is being disclosed as it is necessary to develop the evidential basis. It will enable the identity of the individual suspected of having breached the requirements under the Regulations to be verified, ascertain the period for which the duty will apply, as well as properly and efficiently contact them. This data sharing will also provide information on whether the individual is participating in coronavirus related research, which will be used to determine whether the individual who is suspected to have breached the requirements under the Regulations has done so under an exemption in the Regulations.

b) ‘Notification information’, as set out in section 10.4 provides for sharing of a copy of the notification and includes details as to the legal basis for the duty to self-isolate as well as to confirm the individual was sent a notification to self-isolate and was

aware of their legal duty to do so. ‘Notification information’ will only be disclosed in limited circumstances, for carrying out certain functions under the Regulations. In particular, where this information is required for the purposes of carrying out an enforcement function under the Regulations for the purpose of prevention, investigation, detection or prosecution offences under the Regulations.

This information will allow Police Forces to ensure individuals have been notified to self-isolate and are aware of their legal duty to do so. It also allows forces to provide a copy of the notification to the individual, reminding them of their legal duty to self-isolate.

c) ‘Contextual information’ as set out in section 10.5, provides for the sharing of information regarding how an individual has responded to NHS Test and Trace when contacted. This information includes if an individual has given Test & Trace reasonable grounds to believe that they are not or will not comply with the legal duty to self-isolate, that they were violent, threatening or abusive in their behaviour, or that they indicated they may be vulnerable.

This information will only be disclosed in limited circumstances, for carrying out certain functions under the Regulations. In particular, where this information is required for the purposes of carrying out an enforcement function under the Regulations for the purpose of prevention, investigation, detection or prosecution offences under the Regulations.

This information is necessary, as it will allow Police Forces to inform police risk assessments and to ensure finite resources are used effectively and efficiently.

OGD/External Organisation

3.3 The Police Forces’ powers to share personal data under the Regulations derive from Regulation 14 of the Regulations and the Data Protection Act 2018. There are also powers in section 2A of the NHS Act 2006 and section 115 of the Crime and Disorder Act 1998, as more particularly set out at section 3.2 above. The processing of personal data including its sharing with law enforcement and criminal justice partners and Participants, including to (i) the Crown Prosecution Service, (ii) the ACRO Criminal Records Office (as a data processor for each police force particularly in relation to the issue of fixed penalty notices and their enforcement) (iii) DHSC and (iv) other Police Forces is considered a necessary and proportionate measure to achieve the substantial public interest of preventing danger to public health and thereby ensuring public security in discharge of a policing law enforcement purpose. It also furthers policing law enforcement purposes to prevent and detect crime and bring offenders to justice. In this way, the data sharing facilitates the enforcement of breaches under the Regulations as well as undertaking analysis and reporting work to ensure the ongoing effectiveness of the policing measures in pursuance of a law enforcement process and in so doing, ensures that public security and the trust and confidence in policing is maintained.

4. Lawful basis for processing personal data

4.1 Regulation 14 of the Regulations provides a statutory power to DHSC and Police Forces to use and disclose information as set out in the regulations. There are also powers in section 2A of the NHS Act and section 115 of the Crime and Disorder Act. The Regulation authorises disclosure in cases where there might otherwise have been a duty of confidence or other restriction on disclosure in relation to the information that might prevent that disclosure. Additionally, the police are 'authorised persons' for the purposes of the Regulations to carry out law enforcement activities, including directing or removing a person to return home and issuing FPNs. The Police Forces and DHSC are also required to process data in line with s.149 of the Equality Act 2010 (the Public Sector Equality Duty) and also have common law powers, including in relation to protecting life, preventing and detecting crime and bringing offenders to justice that may be relied on where Regulation 14 does not apply. There are also powers in section 2A of the NHS Act 2006 and section 115 of the Crime and Disorder Act 1998, which may give lawful basis to share information not expressly provided for in the Regulations, but is needed in order to effectively enforce and/or monitor the enforcement of the Regulations. These legal gateways will provide the legal powers to process personal data for the purposes of enforcing the regulations, including sharing such data between the Participants.[5]

4.2 Any processing of personal data using the powers identified must also comply with the UK GDPR and, where necessary, the Data Protection Directive regarding criminal justice processing (EU 2016/680), as implemented by the Data Protection Act 2018. To this end, DHSC will share data under Article 6(1)(e), Article 9(2)(h) and (i) UK GDPR, and Schedule 1, Part 1, paragraphs 2 and 3 Data Protection Act which together provide a lawful basis under the UK GDPR for processing necessary for the purposes of the provision or management of health or social care services, or necessary for reasons of public interest in the area of public health. The provision of data for the purposes of ensuring that people comply with public health measures designed to control the Covid-19 outbreak fits within these purposes.

In addition, Article 6(1)(e) UK GDPR, read with Article 10 UK GDPR, and Schedule 1, Part 1, paragraphs 2 and 3 Data Protection Act provides a lawful basis for the processing of data relating to criminal convictions or offences. It is envisaged that such processing will be limited but may, in particular, involve processing relating to the allegations of breach of the regulations. For the purposes of compliance with Article 6(1)(e) in respect of that data, processing will be carried out under the control of official authority by reason of regulation 14(2)(a)(iv) of the Regulations and will also meet a relevant condition authorising that processing as set out in Schedule 1 to the DPA (processing necessary for reasons of public interest in the area of public health).

4.3 The Police Forces will process personal data, pursuant to section 35(2)(b) and section 35(3)-(5) and Schedule 8, paragraph 1 of the Data Protection Act 2018, which provides a lawful basis for the processing of personal data pursuant to Part 3 Data Protection Act 2018, where the processing of personal data and special categories of personal data for a law enforcement purpose is necessary to give effect to that purpose. In the event that data processing falls outside section 35(2)(b)

[5] Examples of where this may apply include a Police Force providing personal data to DHSC following a 101 call in order to identify whether a person should be self-isolating or not.

and section 35(3)-(5) of the Data Protection Act 2018, the Police Force controlling the information will identify the grounds under which data is processed in accordance with Articles 6, 9 and 10 of the UK GDPR and paragraphs 2 and 3 of Schedule 1, Part 1 Data Protection Act.

5. Privacy Information Notices

5.1 Each Police Force's Privacy Information Notice is set out at Annex C.

5.2 DHSC's Privacy Information Notice is available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/923729/dhsc-privacy-notice.pdf

6. Third Party Processing

6.1. The Participants may use third party processors to process personal data obtained under this PMoU. The Participants will ensure that personal data processed by third party processors is in accordance with the Data Protection Legislation; that personal data will be securely transmitted; that it will take steps to confirm that the third party processor has adequate security arrangements and data storage policies in place; and that only authorised personnel of the third party processor who hold appropriate security clearance are authorised to process the personal data.

6.2 DHSC will undertake due diligence to ensure that no information that can identify a serving Police Officer or Police Staff member will be shared with any third party by DHSC without the prior permission of the Police Force to whom the Police Officer or Police Staff member belongs (as applicable).

7. Data Protection Impact Assessment (DPIA)

7.1. Each Police Force will comply with Data Protection legislation, including, as required by such legislation, the preparation of a bespoke DPIA to document the data protection risks associated with the processing of the personal data to which this PMoU relates. The bespoke DPIA of each Police Force will be in place prior to any data processing taking place under this PMoU, but in the event that a Police Force, as an individual data controller, concludes that a DPIA is not legally required prior to any processing of personal data, they will notify DHSC (at [redacted]) as to that decision and will engage with DHSC as to why the conclusion has been reached that such a DPIA is not necessary. Police Forces should also have regard to any requirement for an Appropriate Policy Document.

7.2. In accordance with DHSC policy, a bespoke DPIA to which this PMoU relates has been prepared.

8. Controller status of the receiving participant

8.1. Each Police Force listed at Annex C and DHSC are independent data controllers for the personal data to which this PMoU relates.

9. Purpose and benefits of the information sharing

9.1. Infectious diseases such as COVID-19 present a serious and ongoing threat to the nation's health. If not controlled, they can infect large numbers of people and, depending on the disease and other factors, can result in ill-effects ranging from relatively minor symptoms to early death. Contact tracing is an important way of controlling the spread of infectious diseases. It is a routine public health practice that involves identifying and tracing all the people who have been in contact with a person who has been infected. Depending on the nature and duration of the contact, these contacts may require advice or treatment to prevent the disease from spreading further, and this may include minimising contact with others.

9.2. The personal data collected by DHSC of a person who tests positive for COVID-19 and their close contacts is covered by the DHSC Privacy Notice Test and Trace: overarching privacy notice - GOV.UK (www.gov.uk). This personal data will be processed by DHSC to support the rapid identification of the contacts of an infected person in order to notify these contacts that they should self-isolate and to provide other advice.

9.3 The sharing of personal data by DHSC to enable the Police Forces to issue fixed penalty notices and/or to enforce self-isolation under this PMoU is considered a necessary and proportionate measure to achieve the substantial public interest of preventing danger to public health and thereby ensuring public security. Police forces may use the personal data to deal with breaches of the Regulations bought to their attention or in the course of their duties. The Police Forces will each enforce the self-isolation as is necessary, proportionate and in accordance with the law (the breach of the requirement to self-isolate is a criminal offence, punishable by fine or the issue of a fixed penalty notice).

Some of the personal data provided is classified as 'special category data' and processing of this type of personal data has to be strictly necessary for the purpose of enforcement as set out in the associated regulations. In this case, this special category data is data which relates to a person's health, in particular, the un-redacted notification and whether the person is under a duty to self-isolate because they tested positive or because they are a contact i.e. the notification information. The contextual information i.e. information about whether a person was recorded as violent, threatening or abusive, or vulnerable, or whether they indicated they would not or are not complying with a duty is also so treated.
It should be noted that there is no bulk data sharing with Police Forces as a result of this agreement. Police Forces will only submit a request for data sharing where they have reasonable suspicion that an individual is breaching the self-isolation legal duty.

10. Information to be shared and the systems the information will be derived from

10.1 To the extent it is necessary for a Police Force (of those listed at Annex C) to further their law enforcement purposes in connection with the requirements imposed by the Regulations, the personal data comprising 'relevant information' to which this

PMoU relates will be collected by the Police Force and provided to DHSC. Such 'relevant information' includes the following details:

a) first name;
b) surname;
c) gender (where requested and provided where held);
d) date of birth (where requested and provided where held);
e) address, including the following information:
    i) property name/number
    ii) street
    iii) town/city
    iv) county
    v) postcode

10.2 To the extent it is necessary for a Police Force (of those listed at Annex C) to carry out their law enforcement purposes in connection with the requirements imposed by the Regulations, the personal data comprising:

a) 'relevant information'; and
b) 'notification information'; and
c) 'contextual information',

which this PMoU related and is collected by DHSC and held on the Contact Tracing Database will be provided to the Police Force.

10.3 'Relevant information' includes whether an individual should be self-isolating or not. The Self-Isolation Regulations make clear that 'relevant information' may only be disclosed for the purposes of carrying out a function under these Regulations, such as to ensure compliance with the legal duty to self-isolate or to prevent danger to the health of the public as a result of the spread of infection or contamination of coronavirus. 'Relevant information' includes the following details:

a) first name;
b) surname;
c) date of birth;
d) gender;
e) telephone number (where held);
f) email address (where held);
g) home and/or self-isolation address (where held), including the following information:
    i) property name/number
    ii) street
    iii) postcode
h) the date on which the individual was sent the notification from NHS Test and Trace to self-isolate;
i) the means by which that notification was given, and the postal address, telephone number or email address (as the case may be);

j) the particular period in respect of which the individual is required to self-isolate;
k) details of any Fixed Penalty Notices issued or contemplated or prosecutions taken under the Regulations;
l) whether the individual is participating in coronavirus related research (where held;
m) a copy of the notification with the information given but redacted to remove information in paragraph 10.4.a.

10.4 'Notification information' may only be disclosed, used and further disclosed for the purposes of carrying out enforcement functions under the regulations, or otherwise for the purposes of the prevention, investigation, detection or prosecution of offences under the regulations and includes:

a) whether the individual is under a duty to self-isolate because they have tested positive for COVID-19, or because they have come into close contact with someone who has;
b) a copy of the notification as sent.

10.5 'Contextual information' may only be disclosed, used and further disclosed for the purposes of carrying out enforcement functions under the regulations, or otherwise for the purposes of the prevention, investigation, detection or prosecution of offences under the regulations and includes:

a) whether when contacted, the individual was violent, threatening or abusive or otherwise behaved in such a way as to make any person carrying on their duties fear for their safety;
b) whether NHS T&T has reasonable grounds to believe that the individual is or would refuse to comply with a requirement to self-isolate and the reasons for that belief;
c) whether NHS T&T has reasonable grounds to believe that the individual is or may be vulnerable, and the grounds for that belief.

10.6 If DHSC becomes aware of a dispute in relation to a notification, in a case where information has already been passed to a police force for enforcement purposes, DHSC will inform the relevant police force of the fact of the dispute as soon as reasonably practicable. The information to be provided is that set out in paragraphs 10.3 -10.5 above, with additional information provided that the case relating to the individual is under appeal. DHSC will notify the police of the outcome of the dispute process as soon as reasonably practicable – i.e. to confirm whether or not the individual was correctly told to self-isolate.

10.7 When notified by a police force that a case is being referred for prosecution and that a witness statement from DHSC is necessary in order to support that prosecution, DHSC will provide such a statement to an evidential standard as soon as reasonably practicable, supported by a statement of truth, along with a copy of the relevant notification and evidence that the notification was given. This will include confirmation that information that has previously been shared with the police under

this clause 10 accurately reflects the records currently held on the Contact Tracing systems. If there is a criminal prosecution (i.e. where the individual does not pay or contests the Fixed Penalty Notice), DHSC will share with the police and Crown Prosecution Service (CPS) evidence of such data as is notified by the police and the CPS as necessary to prove the offence to a criminal standard. The police or law enforcement agency requesting the information will identify the lawful basis for sharing and specify how the sharing meets the test of necessity and (as appropriate) proportionality.

11. Type of information sharing activity

11.1 The personal data listed above is to be shared by DHSC with the Police Forces for their law enforcement purposes until DHSC and the Police Forces (acting through the NPCC) agree that the sharing of the data covering by this PMoU is no longer required.

11.2 If a member of the public has contacted 101, or the police have otherwise been made aware of a concern that someone should be self-isolating the Police Forces have the option to request information from DHSC to establish whether a person should be self-isolating or not.

12. Freedom of Information Act (FoIA) Requests

12.1 Please refer to section 11 of the UMoU for the process of handling FoI Act requests. The Participant that receives a FoIA request will be responsible for responding to that request. The Participant that receives the request must alert the other Participant of the request.

13. Subject Access Requests (SARs)

13.1 Please refer to section 12 of the UMoU for the process of handling SARs.

14. Handling of personal data and personal data security

14.1 Processing under this agreement shall be processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage). The relevant measures shall be recorded in a DPIA where one is undertaken.
Please refer to Section 13 of the UMoU for the protocols of handling personal data securely.

15. General Principles

Accuracy of the shared data

15.1 Before sharing information that includes personal data, the Participants must take all reasonable steps to ensure that the information being shared is limited to

what is necessary and both accurate and up to date in accordance with the Data Protection Legislation.

15.2 Data will be shared on the understanding that the identities of individuals who have been notified to self-isolate will not have been verified by DHSC. The information may therefore be unsuitable to be used as primary evidence without further verification.

15.3 In circumstances where the recipient of the information is intending to use the information to make a decision that will impact directly on the data subject, the receiving Participant must be satisfied that there is sufficient and accurate information available to them before making a final decision and should always seek to clarify, or make further enquiries with the data subject, or with the disclosing Participant in the event that decision is subsequently disputed/appealed by the data subject.

Arrangements for notifying the other Participant of inaccuracies during the information sharing process.

15.4 The accuracy of the personal data provided by DHSC will not be routinely subject to supplementary validation by the Police Forces, but the Police Forces will routinely notify the DHSC contacts at Annex B of any inaccuracies in the supplied data of which they become aware in the course of discharging their enforcement functions.

15.5 If any of the Police Forces becomes aware that personal data is inaccurate, it will notify the DHSC contacts at Annex B as soon as possible and no later than 3 days after it becomes aware of the inaccuracy. DHSC will rectify the inaccuracy within 5 days of being notified by the Police Forces.

16. Data subject's rights

16.1 In the event that a data subject request for access to personal data under Article 15 of the UK GDPR is received by a Participant which relates to personal data held by the receiving Participant under this PMoU, the receiving Participant will process such request in accordance with Data Protection Legislation and will issue a formal response following their internal process and procedures for responding to the requests within the statutory timescales.

16.2 In the event that a Participant receives any other request from a data subject to exercise their rights in connection with the personal data that a Participant holds under this PMoU, the other Participants will where necessary co-operate and assist the receiving Participant to comply with its obligations under the Data Protection Legislation in relation to such a request.

17. Method of information sharing

17.1. The Police Forces, using their PNN or other whitelisted secure email address, and providing the full name of the police officer/staff submitting the request, can

email a request for information on individuals to the DHSC mailbox: [redacted]. DHSC will monitor the mailbox between the hours of 8am to 8pm then reply through the same email route. If relevant information is held then details on the individual, including whether they should be self-isolating or not, will be shared in accordance with this PMoU. DHSC will aim to respond to emails from Police Forces within 24 hours.

18. Retention and destruction schedule

18.1 The personal data to which this PMoU relates will be retained on the DHSC database for 42 days before it is deleted unless still required for a relevant legal purpose that is not incompatible to the original purpose for processing. For example, that personal data will be retained beyond 42 days if the Participants are subject to a legal challenge; or for the purposes of enforcement action.

18.2 The Police Forces will each retain personal data retained until this PMoU in accordance with their relevant retention and destruction policies (including with regards to MOPI and CPIA, as applicable).

19. Permitted uses of the information in respect of this PMoU

19.1 Access to data shared under this PMoU will only be permitted to authorised personnel from DHSC and the Police Forces who have:

- the appropriate security clearance to handle the data for the purposes of this PMoU;
- technical competence to carry out tasks pursuant to the PMoU;
- appropriate training to ensure relevant personnel are aware of the information security policy standards relevant to this PMoU; and
- a genuine business need to access the information.

20. Onward disclosure to third parties

20.1 There will be no routine onward sharing by Police Forces, of the personal data to which this PMoU relates, to third parties, save as set out under the regulations and at Section 3.3. and Section 6 of this PMoU. Police Forces may disclose personal data to third parties where it is necessary to share personal data with law enforcement and criminal justice partners and where it is considered a necessary and proportionate measure to achieve the substantial public interest of preventing danger to public health, and thereby, ensuring public security in discharge of a policing law enforcement purpose.

20.2 DHSC may disclose personal data to third parties where it is necessary to further a law enforcement purpose, to safeguard children and other vulnerable individuals and to assist other organisations in delivering their statutory functions. Any onward disclosure of data obtained by DHSC will only be made in accordance with any applicable legal restrictions, including in particular those contained in the Data Protection Legislation.

20.3 Both Participants agree that any personal data received under this PMoU which is subject to onward disclosure will be securely transmitted, subject to separate written data sharing arrangements and that it will take steps to confirm that the recipient has adequate security arrangements and data storage policies in place.

21. Roles of each Participant to the PMoU

Role of DHSC

21.1 DHSC will provide information to the Police Forces using an agreed format and mailboxes to enable the Police Forces to carry out enforcement functions under the Regulations.

Data processing by DHSC will be subject to the terms of this PMoU and the Data Protection Legislation.

Role of OGD/External Organisation

21.2 Police Forces will each process and provide information to the parties identified at Section 20.1 of this PMoU to carry out enforcement functions under the Regulations, to ensure public health and security and to further its law enforcement purposes.

22. Monitoring and reviewing arrangements

Regular/Routine Exchanges

22.1 This PMoU relates to a regular information exchange and will run for 12 months but must be reviewed within at most 21 days from the date this PMoU takes effect, and then at least every 28 days thereafter, to assess whether the PMoU is still accurate and fit for purpose.

22.2 Reviews outside of the proposed review at section 22.1 can be called by representatives of either Participant. Any changes needed as a result of that review may be approved in writing and appended to this document for inclusion at the formal annual review.

22.3 A record of all reviews will be created and retained by each Participant.

22.4 Annex A and B outline the contacts for amendments to the PMoU, document control, and the version history of the PMoU.

23. Complaints handling/ Issues, disputes and resolution

23.1 Please refer to section 18 of the UMoU for the process of handling complaints, issues, disputes and resolution. Contact details specific to the PMoU are provided at Annex B.

24. Costs

24.1 Each of the Participants shall be responsible for its own costs in relation to this PMoU.

25. Termination

25.1 DHSC, a Police Force (as between itself and DHSC only) or the NPCC (acting on behalf of each of the Police Forces in respect of the all of the Police Forces) (a Terminating Party) may terminate this PMoU by giving a minimum of two weeks' notice to the other Participants. In the event that a Police Force is the Terminating Party seeking to terminate this PMoU, any such termination shall only take effect as between that Police Force and DHSC. The PMoU shall survive as between the other Police Forces, unless terminated by the other Police Forces or the NPCC acting on their behalf.

25.2 DHSC, a Police Force (as between itself and DHSC only) or the NPCC (acting on behalf of each of the Police Forces in respect of the all of the Police Forces) reserve the right to terminate this PMoU in the following circumstances:

- by reason of cost, resources or other factors beyond the control of the Participants;
- if any material change occurs which, in the opinion of the Participants following negotiation significantly impairs the value of the information sharing activity in meeting their respective objectives.

25.3 Where the information sharing relates to a one- off information sharing activity, the PMoU will terminate upon completion of the exercise.

25.4 In the event of a significant personal data breach (see section 22 of UMoU) or other serious breach of the terms of this PMoU by either Participant the PMoU will be terminated or suspended immediately without notice.

26. Personal Data Breaches

26.1 The designated points of contact (provided at Annex A or D (as appropriate) of this PMoU) are responsible for notifying the other Participant in writing in the event of becoming aware of a potential data breach.

Please refer to Section 22 of the UMoU for the process of handling personal data breaches.

27. Signatories

Signed on behalf of DHSC:

27.1 I accept the terms of the Memorandum of Understanding on behalf of DHSC.

Signature:	[redacted]
Name:	[redacted]

Date:	19 March 2021
Position:	Deputy Senior Information Risk Owner for the Department of Health and Social Care

Signature:	[redacted]
Name:	[redacted]
Date:	19 March 2021
Position:	Data Protection Officer for the Department of Health and Social Care

Signed by NPCC on behalf of the Police Forces:

27.2 I accept the terms of the Memorandum of Understanding on behalf the Police Forces.

Signature:	[redacted]
Name:	[redacted]
Date:	19 March 2021
Position:	Chair of the NPCC on behalf of each of the Police Forces

Annex A – Document Control

Document Control Personnel

Key personnel	Name	Organisation (Team)
Author	[redacted]	DHSC
Approver	[redacted] [redacted]	DHSC NPCC
Review Control	[redacted] [redacted]	DHSC NPCC

Version and review history

Version / review	Date	Summary of changes	Changes marked
V1	14/10/2020	PMoU agreed and signed	
V2	30/10/2020	Document formatted for consistency DHSC contacts added 9.2 changed from ‘details of a person taking a test’ to ‘details of a person who tests positive for COVID-19’.	
V3	19/03/2021	Updated to reflect amended regulations, legislative references and the police enforcement process.	

Annex B - Business Contacts

Business as Usual Contacts – DHSC

Contact	Email	Responsibility
DHSC	[redacted]	Complaints Issues/Disputes/Resolution
DHSC Legal	[redacted]	Legal Issues
DHSC FOI	freedomofinformation@dhsc.gov.uk	Freedom of Information
Delivery Lead	[redacted]	Review and amendments to PMoU
DHSC Data Protection Team	[redacted]	Personal Data Breach

Business as Usual Contacts – NPCC

Contact	Email	Responsibility
NPCC	[redacted]	Complaints Issues/Disputes/Resolution
NPCC Legal	[redacted]	Legal Issues
FOI	npcc.foi.request@cru.pnn.police.uk	Freedom of Information
NPCC	[redacted]	Review and amendments to PMoU
NPCC	[redacted]	Personal Data Breach

Escalation Contacts – DHSC

Contact	Email	Responsibility
DHSC	[redacted]	Complaints/ Issues/Disputes/Resolution
DHSC Legal	[redacted]	Legal Issues
FOI	freedomofinformation@dhsc.gov.uk	Freedom of Information
Delivery Lead	[redacted]	Review and amendments to PMoU
DHSC Data Protection Team	[redacted]	Personal Data Breach

Escalation Contacts – NPCC

Contact	Email	Responsibility
Deputy Head of Unit – NPoCC	[redacted]	Complaints/Issues/ Disputes/Resolution
NPCC Legal	[redacted]	Legal Issues
[redacted] Freedom of Information Officer & Decision Maker	npcc.foi.request@cru.pnn.police.uk	Freedom of Information
NPCC Legal	[redacted]	Review and amendments to PMoU
[redacted] NPCC Data Protection Officer	[redacted]	Personal Data Breach

Annex C: List of Police Forces

A list of Forces and their contact details are set out below in the event of any enquiries arising in respect of the data sharing under this PMoU.

Name of police force	Contact, correspondence address and email	Link to Privacy Information Notice
Avon and Somerset Constabulary	The Data Protection Officer Avon and Somerset Constabulary, Police & Fire Headquarters, PO Box 37, Valley Road, Portishead, Near Bristol, BS20 8QJ [redacted]	https://www.avonandsomerset.police.uk/help/privacy/privacy-notice/
Bedfordshire Police	[redacted] Head of Information Management Bedfordshire Police Headquarters Woburn Road Kempston Bedford MK43 9AX [redacted]	https://www.bedfordshire.police.uk/information-and-services/About-us/Privacy-notice/Privacy-intro
British Transport Police	Information Governance Unit 2nd Floor 3 Callaghan Square Cardiff CF10 5BT [redacted]	https://www.btp.police.uk/about_us/your_right_to_information/data_protection.aspx
Cambridgeshire Constabulary	[redacted] Head of Information Management Bedfordshire Police Headquarters	https://www.cambs.police.uk/information-and-services/About-us/Privacy-notice/Privacy-intro

	Woburn Road Kempston Bedford MK43 9AX [redacted]	
Cheshire Constabulary	Data Protection Officer Cheshire Constabulary HQ Clemonds Hey Oakmere Road Winsford Cheshire CW7 2UA [redacted]	https://www.cheshire.police.uk/hyg/fpncheshire/privacy-notice/
City of London Police	[redacted] Director of Information (CISO & DPO) [redacted]	https://www.cityoflondon.police.uk/hyg/city/privacy-notice/ https://www.cityoflondon.police.uk/hyg/cv/coronavirus-covid-19-privacy-notice/
Civil Nuclear Constabulary	Disclosures Officer Civil Nuclear Constabulary Culham Science Centre Abingdon Oxfordshire OX14 3DB [redacted]	https://www.gov.uk/government/organisations/civil-nuclear-constabulary/about/personal-information-charter
Cleveland Police	[redacted] Data Protection Officer Cleveland Police Shared Service Centre Ash House III Acres Princeton Drive Thornaby	https://www.cleveland.police.uk/hyg/fpscleveland/privacy-notice/

	Stockton on Tees TS17 6AJ [redacted]	
Cumbria Constabulary	Force Disclosure Manager/Data Protection Officer People Department, Corporate Support Cumbria Constabulary Police Headquarters Carleton Hall Penrith Cumbria CA10 2AU [redacted]	https://www.cumbria.police.uk/About-this-site/Website-Privacy-Notice.aspx
Derbyshire Constabulary	Data Protection Team Derbyshire Constabulary Butterley Hall Ripley Derbyshire DE5 3RS [redacted]	https://www.derbyshire.police.uk/hyg/fpnderbyshire/privacy-notice/
Devon and Cornwall Police	Data Protection Officer Alliance Data Protection Office, Devon and Cornwall Police Police Headquarters Middlemoor, Exeter Devon EX2 7HQ [redacted]	https://www.devon-cornwall.police.uk/your-right-to-information/data-protection-requests/information-charter-privacy-notice-fair-processing/

Dorset Police	Data Protection Officer Alliance Data Protection Office, Devon and Cornwall Police Police Headquarters Middlemoor, Exeter Devon EX2 7HQ [redacted]	https://www.dorset.police.uk/news-information/legal-privacy/
Durham Constabulary	Data Protection Officer [redacted]	https://www.durham.police.uk/About-Us/Freedom-of-information/General/Documents/Durham%20Constabulary%20Privacy%20Notice%20v5-0.pdf
Essex Police	[redacted] Data Protection Officer Essex Police HQ PO Box 2 Chelmsford CM2 6DA [redacted]	https://www.essex.police.uk/hyg/fpnessex/privacy-notice/
Gloucestershire Constabulary	[redacted] Data Protection Officer Information Disclosure Gloucestershire Constabulary Police HQ 1 Waterwells Drive Waterwells Quedgeley GL2 2AN	https://www.gloucestershire.police.uk/hyg/fpngloucs/privacy-notice/
Greater Manchester Police	The Data Protection Officer Information Compliance and Records Management Unit Greater Manchester Police Information Services Branch	https://www.gmp.police.uk/hyg/fpngmp/privacy-notice/

	Openshaw Complex Lawton Street Manchester M11 2NS [redacted]	
Hampshire Constabulary	Data Protection Officer Mottisfont Court Tower Street Winchester Hampshire SO23 8ZD [redacted]	https://www.hampshire.police.uk/hyg/fpnhc/privacy-notice/
Hertfordshire Constabulary	[redacted] Head of Information Management Bedfordshire Police Headquarters Woburn Road Kempston Bedford MK43 9AX [redacted]	https://www.herts.police.uk/Information-and-services/About-us/Privacy-notice/Privacy-notice
Humberside Police	[redacted] Data Protection Officer Humberside Police Information Compliance Police HQ Priory Road Hull HU5 5SF	https://www.humberside.police.uk/data-protection-privacy-notice
Kent Police	Data Protection Officer Information Security and Governance Department Kent Police Coldharbour London Road	https://www.kent.police.uk/hyg/fpnkent/privacy-notice/

	Aylesford ME20 7SL [redacted]	
Lancashire Constabulary	Data Protection Officer Lancashire Constabulary Police Headquarters PO Box 77 Lancashire PR4 5SB [redacted]	https://www.lancashire.police.uk/information/privacy-notice/
Leicestershire Police	Data Protection Team Information Management Unit Police Headquarters St Johns Enderby Leicester LE19 2BX [redacted]	https://www.leics.police.uk/hyg/fpnleic/privacy-notice/
Lincolnshire Police	Data Protection Officer, Information Management Unit, Police Headquarters, PO Box 999, Lincoln, LN5 7PH [redacted]	https://www.lincs.police.uk/resource-library/data-protection/privacy-notice/
Merseyside Police	[redacted] Data Protection Officer Merseyside Police PO Box 59 Liverpool L69 1JD [redacted]	https://www.merseyside.police.uk/hyg/fpnmerseyside/privacy-notice/

Metropolitan Police Service	[redacted] Data Protection Officer c/o Information Rights Unit PO Box 313 Sidcup DA15 0HH [redacted]	https://www.met.police.uk/hyg/fpnm/privacy/
Ministry of Defence Police	Data Protection Office Room 23, Building 1071 MDP HQ Wethersfield Braintree Essex CM7 4AZ [redacted]	https://www.gov.uk/government/publications/ministry-of-defence-police-privacy-notice/ministry-of-defence-police-privacy-notice
Norfolk Constabulary	Data Protection Officer Norfolk Constabulary Operations and Communications Centre Jubilee House Falconers Chase Wymondham Norfolk NR18 0WW [redacted]	https://www.norfolk.police.uk/about-us/our-data/data-protection/privacy-notice-coronavirus-covid-19
North Yorkshire Police	[redacted] North Yorkshire Police Headquarters North Yorkshire Police Alverton Court Crosby Road Northallerton North Yorkshire	https://northyorkshire.police.uk/access-to-information/privacy-notice/

	DL6 1BF [redacted]	
Northamptonshire Police	Information Unit Manager Force Headquarters Wootton Hall Wootton Hall Park Northampton NN4 0JQ [redacted]	https://www.northants.police.uk/hyg/fpnnorth/privacy-notice/
Northumbria Police	[redacted] Force Data Protection Officer Northumbria Police Schalksmuhle Road Bedlington Northumberland NE22 7LA [redacted]	https://beta.northumbria.police.uk/cookies-and-privacy/
Nottinghamshire Police	Data Protection Officer Information Management Unit Headquarters Sherwood Lodge Arnold Nottingham NG5 8PP [redacted]	https://www.nottinghamshire.police.uk/sites/default/files/documents/files/NottsPrivacy_Notice_25.05.2018.pdf
South Yorkshire Police	Data Protection Officer [redacted]	https://southyorks.police.uk/media/5745/privacy-notice-covid-19.pdf
Staffordshire Police	The Data Protection Officer Staffordshire Police Headquarters Weston Road Staffordshire	https://www.staffordshire.police.uk/hyg/fpnstaffordshire/privacy-notice/

	ST18 0YY [redacted]	
Suffolk Constabulary	Data Protection Team Suffolk Constabulary Martlesham Heath Ipswich Suffolk IP5 3QS [redacted]	https://www.suffolk.police.uk/about-us/our-data/data-protection/privacy-notice-coronavirus-covid-19
Surrey Police	Data Protection Officer Surrey Police PO Box 101 Surrey Guildford GU1 9PE [redacted]	https://www.surrey.police.uk/hyg/fpnsurrey/privacy-notice/
Sussex Police	Data Protection Officer Sussex Police Headquarters Church Lane Lewes East Sussex BN7 2DZ [redacted]	https://www.sussex.police.uk/hyg/fpnsussex/privacy-notice/
Thames Valley Police	Data Protection Officer Thames Valley Police Public Access Office Oxford Road Kidlington OX5 2NX [redacted]	https://www.thamesvalley.police.uk/hyg/fpntvp/privacy-notice/

Warwickshire Police	Data Protection Officer Warwickshire Police Audit, Risk and Compliance Department, PO Box 55 Hindlip Worcester WR3 8SP [redacted]	https://www.warwickshire.police.uk/hyg/fpnwarwickshire/privacy-notice/
West Mercia Police	Data Protection Officer West Mercia Police Audit, Risk and Compliance Department PO Box 55 Hindlip Worcester WR3 8SP [redacted]	https://www.westmercia.police.uk/hyg/fpnwestmercia/privacy-notice/
West Midlands Police	Information Security and Assurance West Midlands Police PO Box 52 Birmingham B4 6NQ [redacted]	https://www.west-midlands.police.uk/about-us/privacy-notice
West Yorkshire Police	[redacted] Data Protection Officer PO BOX 9 Laburnum Road Wakefield WF1 3QP [redacted]	https://www.westyorkshire.police.uk/advice/our-services/your-data/privacy-information-notice/privacy-information-notice
Wiltshire Police	Data Protection Officer Wiltshire Police HQ	https://www.wiltshire.police.uk/media/2289/Wiltshire-

	London Road Devizes Wiltshire SN10 2DN [redacted]	Police-privacy-notice/pdf/Wiltshire_Police_privacy_notice.pdf?m=636802203005570000

www.gov.uk/dhsc