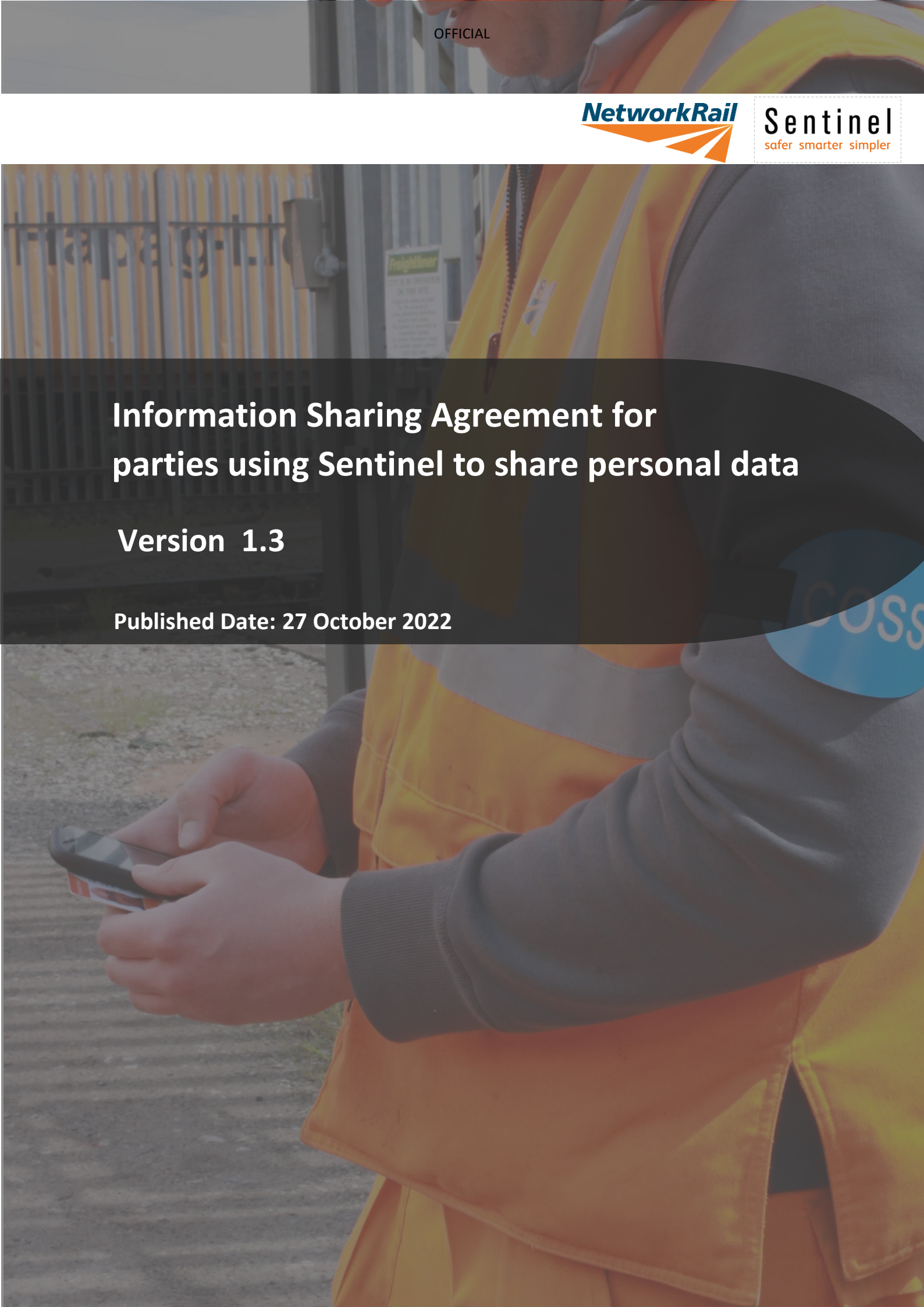

Information Sharing Agreement for parties using Sentinel to share personal data

Version 1.3

Published Date: 27 October 2022

Document Control

Date	Version	Author Role	Author Name	Change Details
27/10/2022	V1.3	Data Protection Specialist	Sandy Gilchrist	Updated with links to forms

Contents

Introduction

This document is an information sharing agreement between Network Rail and each party that uses Sentinel. It governs how Sentinel is used to share personal data, not only between Network Rail and the parties that use Sentinel, but also if parties further re-use Sentinel personal data internally or share Sentinel personal data with other recipients including sub-processors.

Parties must seek approval from Network Rail when using Sentinel personal data by signing this agreement and by completing the appropriate template in the appendices.

The benefits of appropriate information sharing are:

- Better informed decision-making and partnership working for the stated purpose
- Improved data accuracy and relevance to allow a more effective targeting of resources
- Improved health and safety leading to fewer incidents and reduced disruption
- More effective and efficient deployment of resources, activities and processes
- Improved safeguarding of people and infrastructure
- Overall reduction of associated business, security and safety related risks

1. Definitions

Term	Description
Parties	Any organisation that uses Sentinel, e.g. Sponsors, training providers, medical providers, providers of site-access control services, NSAR, and Network Rail, including Technical Authority (the Sentinel custodian that sets out the rules, undertakes assurance assessments, and conducts investigations where required)
Means	the use of Sentinel to process personal data, including information sharing
Purpose	to establish an 'authority to work decision'.
Information sharing	'the disclosure of personal data by transmission, dissemination or otherwise making it available' (§ 121 DPA) – eg viewing, accessing, re-using, sharing, transferring or exchanging it

2. Legislation and Powers

The section describes the legal grounds for Network Rail and each party to share information.

Relevant legislation	Description
Data Protection Act 2018 (DPA) and UK General Data Protection Regulations (UK GDPR)	This sets out the data protection obligations on Network Rail and each party that uses Sentinel to process personal data, including special categories of personal data that in particular require conditions of Schedule 1 of the DPA are met
Human Rights Act 1998	This sets out the obligations on Network Rail as a public authority, in particular Article 8 vis-à-vis information sharing
Common Law Powers of Disclosure	These provide for legal powers for authorities to disclose information, including personal data
Railways Safety (Miscellaneous Provisions) Regulations 1997	These set out the obligations on Network Rail and each party that uses Sentinel to process personal data, including information sharing, in the substantial public interest to meet railway safety requirements
Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS)	These set out the obligations on Network Rail and each party that uses Sentinel to process personal data, including information sharing, in the substantial public interest to meet railway safety requirements
Health and Safety at Work Act 1974	These set out the obligations on Network Rail and each party that uses Sentinel to process personal data, including information sharing, in the substantial public interest to meet health and safety requirements

3. Information Sharing must be Necessary and Proportionate

This section describes the obligations on parties when sharing information, including gaining approval from the Network Rail designated contact by completing the appropriate form.

3.1 Parties may share personal data, provided that:

a) they have notified their intention to do so,
b) the process of information sharing is in accordance with the DPA and UK GDPR,
c) the processing is authorised by law.

3.2 Each party acknowledges that the sharing of information is essential in their legitimate interests for the stated purposes, including identifying and limiting associated business, security and safety related risks and to inform decision-making, projects and activity. Each party must have a documented legal basis for the purposes that it processes personal data.

3.3 The sharing of personal data requires careful judgement in line with DPA, UK GDPR and other legislation, and must be justified on the merits of each case in line with data protection principles. Each party must follow agreed procedures or consult accordingly if in doubt when making decisions about what information to share.

3.4 In considering whether to share personal information each party has a duty to ensure that a fair balance is achieved between the protection of an individual's rights and the general interest of society. In judging whether it is appropriate to share information, each party must examine whether:

a) the stated purpose infringes upon the individual's right to privacy;
b) the appropriate measures to meet the purpose are both fair and rational; and
c) the means used are no more than is necessary to accomplish the purpose.

Similarly, consideration must also be given so that any information shared does not put any of the parties at operational risk. Parties must complete an impact assessment when sharing information.

4. Principles for Information Sharing

This section describes obligations for parties to comply with the data protection principles and to demonstrate compliance to the Network Rail designated contact through the assurance process.

The most important consideration is whether sharing information is likely to support the process meeting the stated purpose.

4.1 Unless an exemption applies the processing of information must be fair. In particular, fairness involves being open with people about how their information is used. Network Rail has made a privacy notice available on the Sentinel website which states how information may be processed and shared. Each party must have and adhere to their own privacy notice.

4.2 Personal data must only be shared for the stated purpose. Any further internal re-use or information sharing with other recipients that is not related to the stated purpose is not permitted. Each party must have ensure that any further intended processing is limited to the stated purpose only.

4.3 When taking decisions about what information to share, parties must consider how much information needs to be released. Not sharing more data than is necessary to be of use is a key element of the UK GDPR and DPA, and parties must consider the impact of disclosing information

on the affected individual(s) and any third parties. Any information considered for sharing must be lawful, accurate, and proportionate to the level of risk in sharing it for the stated purpose.

4.4 Only information that is relevant to the purposes for which it is being shared should be made available to those who need it, with proper reference made to the nature of the source. This allows others to do their job effectively and make informed decisions.

4.5 Information must be adequate relative to the purpose for which it is being shared. Information should be of the right quality to ensure that it can be understood and relied upon.

4.6 Information must be accurate and up to date and clearly distinguish between fact and opinion. If the information is historical then this must be explained.

4.7 Information must be shared in a timely fashion to reduce the risk of missed opportunities to identify and limit business, security and safety related risks associated with the stated purpose and to inform decision-making, projects and activity. Timeliness is key in emergency situations, and it may not be appropriate to seek consent for information sharing if it could cause delays and increase the risk of harm. Parties must ensure that sufficient information is shared, and consider the urgency with which to share it.

4.8 In line with each party's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

4.9 Information sharing decisions must be recorded by each party, whether or not the decision is taken to share. If the decision is to share, a log must cite reasons including what information has been shared, when and with whom, in accordance with their organisational procedures. If the decision is not to share, parties should record the reasons for this decision and discuss them with the requester.

5. Personal Data Breaches

This section describes the requirement for parties to notify other affected parties when there is a personal data breach by completing the appropriate form and to follow any instructions from the Network Rail designated contact.

Any processing, sharing or other disclosure of information by an employee, contractor or other worker which breaches legislation, or this agreement, will be subject to an investigation and where necessary, reported to the Information Commissioner's Office (ICO).

5.1 It is the responsibility for the party with whom the individual is contracted to to contact the ICO regarding any breaches.

5.2 It is the responsibility of each party to notify the other party of any known breach or infringement immediately and remedial action must be agreed and actioned as necessary. Each party will be accountable for any misuse of information and action taken will be in line with disciplinary policies. A breach may result in this agreement being temporarily or partly suspended by either party.

6. Individuals' Right to Exercise Their Rights

This section describes the requirements by parties to deal with requests from individuals to access, modify or erase their personal data, and by gaining approval from the Network Rail designated contact by completing the appropriate form.

A Subject Access Request ("SAR") is an individual's right to have a copy of information relating to them which is processed by a party. Individuals also have other rights.

6.1 SARs and other such requests will be dealt with by the party that receives the request, including where appropriate notifying the other party.
6.2 Each party must assist the other party where reasonably required to do so.

7. Security Arrangements

This section describes the requirements for parties to have appropriate security policies in place, and to gain approval from the Network Rail designated contact by completing the appropriate form.

7.1 Each party should ensure they have and adhere to appropriate security policies in place and arrangements to ensure that personal information is protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
7.2 In accordance with their respective policy on security for handling personal information, each party must establish common rules for shared data security.
7.3 The transfer, use, storage and retention of the information by each party must comply with the DPA and should comply with the security requirements stipulated within this agreement.
7.4 As best practice the disclosing party should make sure that any personal information they disclose will continue to be protected and that the recipient has adequate security measures in place.
7.5 It is essential that each party provide personal or other sensitive information only to specific individuals authorised to receive it, in accordance with the purpose for which it was obtained. have a timescale for assessing the ongoing effectiveness of the data sharing initiative and the agreement that governs it.
7.6 Any additional security requirements that a party wishes to specify must be done so in agreement with Network Rail, subject to the general agreement or its specific data sharing elements as laid down in other arrangements between the parties.

8. Further Internal Processing or Onward Transfers

This section describes the requirements for parties to only re-use personal data for further purposes or transfer to other parties by gaining approval from the Network Rail designated contact by completing the appropriate form.

8.1 Unless a separate agreement is in place, or a statutory requirement for disclosure exists, should either party wish to disclose information that has been shared with them to a third party or to re-use the personal data for further purposes, written consent should be sought from Network Rail or other providing party.
8.2 Each party must ensure that all principles of the DPA are adhered to. Therefore, if further disclosure is made to a third party or the personal data is re-used for further purposes, it must not be incompatible with the stated purpose.
8.3 Where a competent authority legally requests personal data that has been shared, all such requests should be notified to CFIS@networkrail.co.uk..

9. Accountability

This section describes the requirement for parties to be accountable and to follow any instructions from the Network Rail designated contact.

With regards to information sharing, each party must conduct their own assurance assessments and audits on a timely basis for accountability purposes, in particular with regards to data protection by

design and by default, to ensure appropriate policies, processes and procedures are internally in place for information sharing that in particular:

9.1 contain detailed advice about which datasets they can share, including special categories, to prevent irrelevant or excessive information being disclosed;

9.2 set out the lawful basis for each type of personal data being processed, and arrangements for international transfers;

9.3 make sure that the data they are sharing is accurate, for example by requiring a periodic sampling exercise and data quality analysis;

9.4 record data in the same format, abiding by open standards when applicable, including how to record or convert particular data items, for example common industry formats;

9.5 have common rules for the retention and deletion of shared data items, as appropriate to their nature and content, and procedures for dealing with cases where different parties may have different statutory or professional retention or deletion rules;

9.6 have common technical and organisational security arrangements, including the transmission of the data as well as procedures for dealing with any breach in a timely manner;

9.7 ensure their staff are properly trained and are aware of their responsibilities for any shared data they have access to;

9.8 have procedures for dealing with access requests, complaints or queries from members of the public;

9.9 have a timescale for assessing the ongoing effectiveness of the information sharing initiative and the agreement that governs it;

9.10 have procedures for dealing with the termination of the information sharing initiative, including the deletion of shared data or its return to the party that supplied it originally; and

9.11 assign individuals within each party to be responsible for ensuring adherence to this agreement and specific data sharing obligations in particular to agree and monitor the

a) information to be accessed
b) specific processes as set out or referred to in contracts and other arrangements
c) roles and responsibilities as laid down in clause 11 herein.

10. Joint Controllers

This section describes the requirements for parties to comply with joint controller written arrangements, and by gaining approval from the Network Rail designated contact by completing the appropriate form.

10.1 Where the parties are joint controllers in relation to the sharing of personal data, the parties shall be bound by written arrangements regarding their respective duties and tasks to carry out data protection obligations. These must at least include collaborating and agreeing on data protection impact assessments, onward transfers including international transfers, managing rights requests, and adherence to data protection principles.

11. Roles, Responsibilities and Reviews

This section describes the requirements for parties to agree their roles and by gaining approval from the Network Rail designated contact by completing the appropriate form.

11.1 Processing that occurs before the sharing of personal data is the responsibility of the originating party, who will deal with any rights requests relating to such priori processing. Similarly, it is the responsibility of the receiving party to deal with any rights requests in relation to any processing that occurs after the sharing of personal data, including internal re-use or where

there are sub-processors or in the case of onward transfers with other controllers. Joint processing activities including the sharing of personal data is the responsibility of all parties involved.

11.2 Each party shall assign a role to be responsible for ensuring adherence to the principles set out in this agreement.

11.3 Each party shall upon reasonable request make available to the requesting party and authorities such documentation that demonstrates compliance with this agreement.

11.4 After six months of this agreement coming into force, a review will be undertaken to assess the ongoing effectiveness of the data sharing initiative and this agreement, and thereafter every two years.

11.5 A review must also be conducted in the event of a personal data breach if related to joint processing activities such as a failure in security leading to unauthorised or unlawful processing due to the sharing of personal data.

12. Signatures

This section describes the requirements for parties to agree this agreement with Network Rail.

12.1 By signing this agreement, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself is sufficient to meet the purposes of this agreement.

12.2 Signatories must also ensure that they comply with all relevant legislation.

12.3 It is the responsibility of all signatories to ensure that:

a) realistic expectations prevail from the outset.
b) professional and ethical standards are maintained.
c) the data protection principles are upheld, in particular access controls.
d) the information exchanged is kept secure and confidentiality is maintained as appropriate to the information's level of protective marking as defined by the controller.
e) a mechanism exists by which the flow of information can be controlled.
f) appropriate staff training is provided on this agreement.
g) they have the appropriate authority to sign this agreement,

13. Approvals

At the time of accessing Sentinel, this agreement is in force in line with Sentinel T&Cs and in conjunction with the Sentinel Scheme Rules.

Content	Network Rail Infrastructure Limited	Party exchanging Sentinel data with Network Rail
Organisation	Sentinel Operations Team	Primary Sentinel contact (unless otherwise stated)
Date of authorisation	Effective 31 October 2022	Effective 31 October 2022

14. Appendices

Appendices #	Document
1	Information Sharing Request Form
2	Information Sharing Decision Tree
3	Information Sharing Decision Form