



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

Freedom of Information Act Publication Scheme	
Government Security Classification	Official
Publication Scheme Y/N	Yes
Title	A purpose specific Information Sharing Agreement (ISA) between National Vehicle Crime Intelligence Service (NaVCIS) and Tracker Network (UK) Ltd.
Version	1
Summary	An agreement to formalise data sharing arrangements between National Vehicle Crime Intelligence Service (NaVCIS), Tracker Network (UK) Ltd and High Mobility **S31(1)**
(B)OCU or Unit, Directorate	National Vehicle Crime Intelligence Service (NaVCIS)
Author	DCI Brett Mallon
Review Date	
Date Issued	20/07/2023
Cyc freedom Ref	

Purpose Specific

Information Sharing Agreement (ISA) Between NaVCIS National Vehicle Crime Intelligence Service (NaVCIS), Tracker Network (UK) Ltd and High Mobility



Table of Contents

Section 1:	Purpose of the Information Sharing Agreement	Page 3
Section 2:	Background and data to be shared	Page 4
	• Purpose and scope for sharing data • Data to be shared	
Section 3:	Privacy Management & Security Framework	Page 10
	• Data sharing process • Confidentiality and vetting • Data Transfer • Data storage • Business Continuity • Data destruction / disposal • Retention • Reporting Security incidents & breaches to the Agreement • Compliance • Review	
Section 4:	Legal bases for sharing data	Page 17
	• First Data Protection Principle: Lawful Gateway • Human Rights Act (1998) • Data Protection Act • Data Protection Principles • Consent • Common Law Duty of Confidentiality • Freedom of Information and Right of Access Requests	
Section 5:	Agreement signatures	Page 26
Appendices		
	A Data Protection Principals	Page 27
	B Evidence of Consent	Page 29

NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICETrackerTMOfficial

This Information Sharing Agreement is for Law Enforcement purposes only. Under Part 3 of the Data Protection Act (2018), NaVCIS qualifies as a competent authority for the purposes of: “the prevention, investigation, detection or prosecution of criminal offences; or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.”

Section 1. Purpose of the Information Sharing Agreement

The purpose of this ISA is to agree formally how Personal and / or Special Category Data shared between NaVCIS and Partner Organisation(s) will be processed and used.

By signing this agreement, the named agencies agree to accept the conditions set in this document, according to their statutory and professional responsibilities. They also agree to adhere to the procedures described herein, which are to:

- Define the specific purpose(s) for which the Signatory Organisation(s) have agreed to share data;
- Outline the Personal and or Special Category Data to be shared;
- Set out the legal gateway through which the data will be shared;
- Stipulate the role(s) and procedures that will support the processing of data between the Signatory Organisation(s);
- Describe how the rights of the data subject(s) will be protected as stipulated under the following Data Protection laws: General Data Protection Regulations (GDPR), Law Enforcement Directive and the Data Protection Act (2018);
- Describe the security procedures in place to ensure compliance with the Data Protection Act (2018) and Partner Organisation(s)-specific requirements;
- Describe how the Signatory Organisation(s) will monitor and review this arrangement.

The signatories to this agreement will represent the following agencies:

- National Vehicle Crime Intelligence Service (NaVCIS) and
- **Tracker Network (UK) Ltd** (also referred to as ‘Tracker’)



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Section 2. Background to initiative and what information you plan to share

2.1 Purpose and Scope for sharing data

Q1. Provide the background to this initiative and explain what this project is about:

NaVCIS is a national police unit supporting the National Police Chiefs Council (NPCC) national vehicle crime portfolio.

Its purpose is to work collaboratively across policing and industry to:

Prevent and detect vehicle finance crime, theft of plant and agricultural machinery, freight crime and the theft of leisure vehicles.

Collate, analyse and disseminate data and intelligence to benefit police and industry.

NaVCIS provides intelligence and law enforcement services in support of counter fraud activity against the UK Finance and Leasing Association members. NaVCIS is privately funded by some, but not all, FLA members and acts primarily in their interest however does provide a number of additional vehicle crime and intelligence services throughout the UK.

This support given by NaVCIS includes utilising on-board telematics or tracking systems, to facilitate the recovery of vehicles that are stolen or being used by persons whose life is at risk (such as high risk missing persons).

A long-term partner in this stolen vehicle recovery (SVR) is Tracker Network (UK) Ltd.

Tracker Network (UK) Ltd (Tracker)

Tracker Network (UK) Ltd have been operating as a Stolen Vehicle Recovery (SVR) business in the UK since 1993; UK Policing, via ACPO and Police Authorities, agreed to formally collaborate with Tracker. This included an agreement with every Police Force in England and Wales, Scotland and to a lesser extent the Royal Ulster Constabulary (now PSNI).

The agreement included the sharing of information on a daily basis between individual Police Forces and Tracker in support of Law Enforcement and via NaVCIS latterly after the introduction of the Unit.

Over the past 30 years Tracker and the Police have recovered stolen vehicles close to the value £600m and Tracker have significantly supported Law Enforcement in providing information and intelligence in bringing offenders to justice, in support of many serious crime investigations and also in helping to locate and protect vulnerable people (particularly those with suicidal tendencies).

****S31(1)****



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Q2. Explain briefly what this project aims to achieve:

This aim of this project is to:

****S31(1)****

For many years, Tracker have worked closely with a number of vehicle original equipment manufacturers (OEM's) many of which have installed telematics systems to their vehicle at the time of production.

****S31(1)****

Q3. Confirm what type of data you will be using i.e. Personal and or Special Category¹:

The data shared will typically not be Personal data, or at most will only be able to identify a person through a secondary (police) intelligence system.
No special category data will be shared.

Q4. Provide a clear list of the data that Tracker is requesting from NaVCIS and label which ones are Personal and or Special Category Data:

e.g. information on crimes, terrorism, anti-social behaviour and public order

In relation to identified stolen vehicles, or on police request for vehicles used by persons whose life is at risk -

- Vehicle Registration number (Personal data)
- Vehicle Make and model (Not personal data)
- Vehicle VIN/ Chassis number (Not personal data)
- Police force where the vehicle was stolen (Not Personal data)
- Police Crime number (Not personal data)
- Date of theft (Not personal data)
- Insurance company detail (or stating if insurance not held) (Not personal data)
- Date last insurance held and/or reason for no insurance if known (Not personal data)

¹ **Personal Data:** Data relating to a living identified or identifiable individual, including: a person's name, address, dob, email address, telephone number, id number, bank and credit card details, location data, online identifier or one or more factors specific to someone's physical, physiological, genetic, economic, cultural or social identity.

Special Category Data: Data that reveals a person's racial, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, biometrics, health, sex life / orientation, criminal convictions and offences, related security measures or appropriate safeguards. This includes photographs and CCTV images.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

Q5. Provide a clear list of the data that NaVCIS is requesting from Tracker and label which ones are Personal and or Special Category Data:

Tracker will forward the identified VIN numbers to the data handler partner, who will share this with the OEMs.

****S31(1)****

Installed with the capability to provide movement and location data. (No personal data exchanged)

This list of viable vehicles will be provided to NaVCIS. (Not personal data)

After completion of checks and activation (*see full process outlined in question 36*), the data handler will obtain the **vehicle location** (or report on the system being inactive if relevant), and pass this to Tracker who will provide it to NaVCIS for police action.

(Vehicle location is not typically personal data – as checks ensure only unrecovered stolen vehicles are so located; and the location of the vehicle whilst with criminals is not protected data. When the location is requested by police for life at risk - this is personal data.)

Q6. Explain the benefits of this sharing agreement for:

NaVCIS:

- Crime, disorder, vulnerability and harm are prevented, disrupted and reduced.
- Improvement in security.
- Improvement in public confidence.
- Offenders are identified and brought to justice.
- Delivering performance by focussing the priorities on the communities need
- Increasing NaVCIS presence by adding value to work with partners and agencies.
- Supporting police to find and protect vulnerable persons

b) Tracker Network (UK) Ltd

- Supports the Tracker partnership of supporting law enforcement
- Provides a potential income stream through fees agreed with insurers of the recovered stolen vehicles.

The Public:

- Ensuring the prevention and detection of crime.
- Reduce the fear of crime or criminal activity.
- Facilitate value for money and cost-effective solutions.
- Ensure public confidence that there are systems in place to stolen vehicles.
- Maintain the economic wellbeing of the United Kingdom.
- Deter criminals from stealing vehicles
- Protecting life and vulnerable persons



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

2.2 NaVCIS Data to be shared

Q7. List the NaVCIS system(s) the data will be taken from and the relevant fields in these systems you intend to use:

*i.e. **CRIS** – name, address, details of investigation found on DETs page, **PNC** - disposable history.*

NaVCIS will obtain regular lists of vehicles stolen across the UK from **the Police National Computer (PNC)**. (And actively search PNC for a specific vehicle, for threat to life requests.)

- Vehicle Registration number (Personal data)
- Vehicle Make and model (Not personal data)
- Vehicle VIN/ Chassis number (Not personal data)
- Police force where the vehicle was stolen (Not Personal data)
- Police Crime number (Not personal data)
- Date of theft (Not personal data)
- Insurance company detail (or stating if insurance not held) (Not personal data)
- Date last insurance held and/or reason for no insurance if known (Not personal data)

Q8. State the reason(s) why it is necessary to share this data with the Partner Organisation(s) and what the impact would be if it was not shared:

The initial sharing of data provided by NaVCIS is only a list of VINs, for vehicles listed on PNC as stolen (or a specific vehicle with a threat to life request, originating from the police.)

This data can only be provided from police systems.

This list needs to be checked by the OEMs ****S31(1)**** ; this data is only held by the respective OEMs. Tracker and the Data handler third party is required to manage to contact with the respective OEMs, who will not share such information outside of specific agreements with agreed partners.

The OEMs will then reply with the identified potential vehicles, for the next stages of the process with Tracker and NaVCIS.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Q9. Please confirm the following:

Tracker Network (UK) Ltd will not disclose NaVCIS data shared under the terms of this agreement with a third party without first seeking the permission of NaVCIS unit that provided it.

Yes.

The data handler used by Tracker will be High Mobility, based at; Immanuelkirchstrabe, 8A, 10405, Berlin, Germany.

The OEMs involved are listed by Tracker, who will update NaVCIS as members join or leave.

If the answer is no, please explain why:

Q10. If a third party will access NaVCIS data, then the NaVCIS deputy Head of unit will need to know about the process used to make it available to them and how they will process it.

If this question applies, please explain how this data will be shared with a third party and what that party will do with it:

This scenario is not anticipated with this agreement.

However, operational policing allows case by case decisions and in the unlikely event that such extra sharing is needed to save life or 'other serious reason', a fast time decision on sharing will be made by NaVCIS, or other police force if working directly with Tracker. That will be covered under normal data sharing rules, decided upon using national policing principles, UK legislation and recorded as such by the officer deciding.

Q11. Will NaVCIS data shared under the terms of this agreement remain within the European Economic Area (EEA)?

Yes

If the answer is no, explain how you will safeguard any international transfers:

2.3. Consent

Explicit consent must be sought from data subjects where it has been identified as necessary for the processing of personal data, as stipulated in the relevant Data Protection, GDPR, Law Enforcement Directive legislation, and policies of the Partners of this agreement.

Where consent is required, it is the responsibility of the Partner Organisation(s) to seek it from the data subjects. Individuals should be made aware of how their personal data will be processed, why and which agencies it will be shared with. They should also be informed that they can withdraw their consent at any time.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

In circumstances where consent has been refused or withdrawn by the data subject, that data must not be used, unless withholding it would risk causing harm or distress to another party. Nevertheless, there may be occasions where personal data may be legally shared with other agencies without consent.

Q12. Please confirm the following:

Tracker will seek the explicit² consent of its data subjects:
Delete as appropriate

Yes

If the answer if no, please explain why:

Initially minimal data is shared from policing systems to third parties (VINs) and only for confirmed stolen vehicles. Once viable vehicles are established the host forces and insurance companies will be contacted and only with the consent of appropriate party (vehicle owner, or insurance company) will any location data be sought or provided.

If the answer is yes, explain how explicit consent will be sought, providing evidence if applicable: *i.e. attach a copy of the consent form you used to the appendix of this DSA or provide the wording given to data subjects in order to obtain their consent.*

Q13. Please confirm the following:

Tracker Network (UK) Ltd client's data subjects have been made aware of how their personal data will be processed.
Delete as appropriate

Yes

If the answer is yes, please explain how the Partner Organisation(s) made them aware and if the answer is no, explain why:

The initial data sharing of VINs by NaVCIS and then the approach to police forces and insurers with the crime number is without consent of the data subject, no personal data is shared other than the VRNs (which is only able to identify a data subject with a police system); after that stage consent will have been obtained, i.e., where vehicle Insurer details are known (held on PNC), consent will have been secured from the Insurer ****S31(1)**** If Insurer details are not known (not held on PNC) or where the specific Insurance company has not provided consent, attempts will be made

² Under the Data Protection Act (2018) consent must be obtained by a participant opting in. It cannot be implied or assumed and it must be for a specific purpose.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

to contact the current registered keeper of the vehicle (via the Police) and consent will then be sought from the keeper/owner of the vehicle in order to then activate the vehicles telematics device.

In the event that there is no consent from either the vehicle Insurer or current vehicle keeper/owner, attempts will not be made to activate the vehicles telematics device.

2.4. Common Law Duty of Confidentiality

If information is provided in confidence to one of the signatories of this agreement then they have a Duty of Confidentiality towards the data subject that it concerns and can only share this information if they have a compelling reason (i.e. in the public interest) to do so.

Q14. Confirm the following:

The Partner Organisation(s) has a duty of confidence towards its Clients:

Delete as appropriate

Yes

If the answer is yes, explain what legal reason they would use to justify disclosing this data to a third party:

Through contractual agreements.

3. Privacy Management & Security Framework

3.1 Data Sharing Process

Requests for NaVCIS data

Q15. Please explain the following:

a) How will the Partner Organisation(s) make requests for NaVCIS data?

NaVCIS will routinely provide regular list of stolen vehicle VINs to Tracker; follow on information will be as per the agreed process.

Any clarification or unusual requests will be made by emails and record of data exchanges is to be kept.

Urgent requests can be made by telephone, but followed up by an email outlining that agreed and shared.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

b) Who [job title] within the Partner Organisation(s) is responsible for making these requests?

NaVCIS will forward data to Clive Wain – Head of Police Liaison, Tracker

c) State the means by which these requests will be made:

i.e. via secure (state the type) email, post, phone:

NaVCIS will forward all data and intelligence to the above named person via Email.
(Phone requests are acceptable if an email request is subsequently provided for NaVCIS records.)

Q16. How will NaVCIS gather the data requested?

The partnership between NaVCIS and Tracker is not changed by this latest agreement and Tracker can act on the stolen vehicle VIN data routinely provided; this agreement provides permission for Tracker to share that data with third parties for the reasons outlined above.
The trial period agreed is for 3 months.

Q17a. Who is NaVCIS primary point of contact [job title] within the Partner Organisation(s)?

Clive Wain

b) Who are [job title] the recipient(s) of NaVCIS data within the Partner Organisation(s)?

- Head of Police Liaison, Tracker

c) If there is a secondary point of contact, state who [job title] it is?

- Steve Whittaker –Tracker Police Liaison Manager

Q18. Is there a requirement for the Partner Organisation(s) to have access to NaVCIS ICT systems?³

Delete as appropriate

No

If so, state which systems, who [job title] specifically will have access to them and why they require it:

n/a

³ This should only happen when it is operationally imperative to share data and there is no other means available. If access will be granted to personnel from a Partner Organisation, please include the following text: "All usage of NAVCIS systems will be audited in line with NAVCIS and national standards. NAVCIS managers will ensure a suitable level of supervision is provided".



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Requests for Tracker Network (UK) Ltd Data

If the NaVCIS will also receive data from the Partner Organisation(s) then complete the following section.

Q19. Please explain the following:

a) How will NaVCIS request data from the Partner Organisation(s)?

Provision of location data on actively sought vehicles will be sent via secure email.

The nature of the requests can be discussed by phone, but the formal request will be via email.

b) Who [job title] is responsible for making these requests?

NaVCIS supervisor or Vehicle Location Enquiry staff

c) State the means by which these requests will be made:

i.e. via secure (state the type) email, post or phone.

Email will be primary request. Phone calls are acceptable if urgent, but to be confirmed in an email.

Q20a. How will the Partner Organisation(s) gather the data requested?

Tracker will obtain location details on subject vehicles, via their data handler, who will be the primary contact with the OEMs.

b) Who [job title or name of unit] will be responsible for doing this?

High Mobility
Immanuelkirchstrabe
8A, 10405
Berlin
Germany

c) Which systems will be interrogated?

N/A

Q21a. Who is the Partner Organisation(s)'s primary point of contact for NaVCIS?

Clive Wain

b) Who [job title] are the recipients of the Partner Organisation(s)'s data within NaVCIS?

- Head of Police Liaison, Tracker



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

c) If there is a secondary point of contact, state who [job title] it is?

- Steve Whittaker – Tracker Police Liaison Manager

The **NaVCIS SPOC** will create a record of any personal data disclosed to Tracker Network (UK) Ltd on GSA, at the time the data is supplied (or as soon as possible thereafter). This should include what was shared or not, and the reason for that decision.

3.2 Confidentiality and Vetting

Where OFFICIAL SENSITIVE data is being shared, vetting is not mandatory but access must be, limited to those that “need-to-know” (unless there are national security implications, in which case a Counter Terrorist Check (CTC) is required). Tracker Network (UK) Ltd must confirm that employees who will access shared data will have a genuine “need-to-know”, and that they have provisions in place to ensure that unauthorised dissemination or copying by their staff does not occur.

Q22. Have employees in the Partner Organisation(s), who receive NaVCIS data, undergone any vetting?

No

If so, please state to what level:
i.e. CTC cleared

Q23. Does the Partner Organisation(s), require their employees to sign a confidentiality agreement, or an equivalent level of assurance of confidentiality?

Delete as appropriate

Yes

If the answer is no, please explain why such measures are not required:

n/a

3.3 Data Transfer

Hard Copy

- A trusted person will move the data, in a closed container or package.
- Data will be moved by post or courier, in a sealed package with no security classifications showing (other than Personal or Private). It will be addressed to Clive Wain at Tracker Network (UK) Ltd.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

Electronically

- Data marked with a Government Security Classification up to the level of OFFICIAL SENSITIVE will be transferred using '.police.uk' and CJSIM secure email.
- If information is to be shared over the telephone, speech will be guarded and conversations kept short.

Data transfer over fax is prohibited, as it is not secure.

3.4 Data Storage

Partner Agency's Building & Perimeter Security

NaVCIS data must be kept within a secure location with a managed and auditable access control system that the general public will have no access to.

Hard Copy

Q.24. Explain how the Partner Organisation(s) will store hard copies of OFFICIAL SENSITIVE NaVCIS data:

Tracker will not store hard copies of the NaVCIS data

Electronically on a Partner's system

Q25. Explain what system access controls the Partner Organisation(s) has in place to keep NaVCIS information safe:

NaVCIS information will be kept in an encrypted location and only specified staff at Tracker will be granted access to it.

- Official Sensitive NaVCIS information will be stored in a locked container within a secure premise with a managed access control. Access to information will be limited to those with a genuine "need to know". When the documents are not being used they will be locked away.

Partner Organisation have established and implemented Information security management systems policy as part of the ISO-27001 framework

Annual audit June 2022

3rd party vendor – yearly penetration tests

All communication to and between our services and resources is SSL encrypted - Domain validated (DV), organization validated (OV), extended validation (EV)

Tracker has ISO accreditation related to call handling but do not have ISO27001 certification currently.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Q26. Tracker Network (UK) Ltd confirm that the NaVCIS data they hold can be audited at any time.

Yes – by prior arrangement

If the answer is no please state why:

n/a

Q27. Tracker Network (UK) Ltd is part of the UK Government Cyber Essentials scheme.
Delete as appropriate

No

If the answer is yes, please provide the date when they joined:

n/a

3.5 Business Continuity

If the data shared within this agreement will be backed up, either electronically or with the movement of physical files, then the responsible party must ensure that the appropriate storage and protection measures are in place.

Electronically

If data is backed up electronically via a hard drive, or any mobile device, then the appropriate level of encryption and or password requirements must be in place. This device should also be stored in a physical location with the same level of security as the data being held.

Hard Copy

If data shared under this agreement must be moved from its usual secure location, which is in accordance with the level of security required by this agreement, then any move temporary or permanent must provide the same level of security in storage as originally agreed and stated in this document.

Whilst the Partner Organisation(s) may have their own security standards & protocols, where NaVCIS data is concerned the relevant security standards set out by the GSC for transmitting, storing and disposing data must be adhered to at all times.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

3.6 Data Destruction / Disposal

Hard Copy

- Papers will be disposed of through an OFFICIAL SENSITIVE waste system.
- Papers will be disposed of using a cross shredder.
- Papers will be returned to NaVCIS premises for disposal.

Electronic Information from Partner's System

- Electronic data held on a Partner Organisation's system will be securely erased or overwritten using an approved software utility to a standard applicable to the Government Security Classification.
- Electronic data will be disposed of through the physical destruction of the computer media.

3.7 Reporting Security Incidents and Breaches of the Agreement

Partner Organisation(s) Responsibility

Security breaches, including misuse of NaVCIS data, must be reported to the NaVCIS deputy head of unit without undue delay of occurring/or no later than 24 hours after the Partner Organisation(s) becomes aware of it. This is to allow the NaVCIS to risk assess the security incident or breach of this Agreement.

Contact to NaVCIS on email: intel@navcis.police.uk

The nominated NaVCIS SPOC will also immediately inform the NaVCIS deputy head of unit, who will inform the Hampshire Constabulary Joint Information management Unit (JIMU) of any security incidents or breaches of this agreement, including unauthorised disclosure or loss of data, by emailing. 'information.governance@hampshire.police.uk'; or using the Hampshire intranet portal 'Report a security incident'

However it is still the responsibility of Tracker Network (UK) Ltd to comply with the obligations laid out under Section 67 and 68 of the DPA 2018.

It is also confirmed that security breaches including misuse or unauthorised disclosure, are covered by Tracker Network (UK) Ltd internal disciplinary procedures. If misuse is found, there should be a mechanism to facilitate an investigation, which includes initiating criminal proceedings where necessary.

NaVCIS Responsibility

Q28. Detail the process **Tracker Network (UK) Ltd** would like NaVCIS to comply with should a security breach occur on our part:

Contact Clive Wain, or Steve Whittaker at Tracker within 24 hours of the security breach by telephone and email.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

3.9 Compliance

All partners are responsible for ensuring that security controls are implemented and staff are aware of their responsibilities under the Data Protection Act 2018.

All partners agree where necessary to allow peer-to-peer reviews to ensure compliance with the security section of this DSA. Compliance with these security controls will be catered for in the periodic reviews of this DSA.

3.10 Review

In accordance with the Guidance on the Management of Police Information (MoPI) this ISA will be reviewed six months after implementation and annually thereafter.

Section 4: Legal basis for sharing data

Section 4 of this ISA explores the legality of sharing data. It details how this agreement will comply with the relevant Statutory or Common Law powers when sharing data with the Partner Organisation(s).

4.1 Human Rights - Article 8: The Right to Respect for Private and Family Life, Home and Correspondence

Article 8 says:

- (1) Everyone has the right to respect for his private and family life, his home and his correspondence.**
- (2) There shall be no interference by a Public Authority with the exercise of this right, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.**

However, this is not an absolute right and when weighed against the public interest, it may be justifiable to interfere with this right.

Q29. Show below how this Information Sharing Agreement is:

In pursuit of a legitimate aim: *e.g. preventing or reducing crime – under Statute or Common Law*

This ISA will help to prevent and detect crime, recover stolen property and bring offenders to Justice under Common Law.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Proportionate:

This agreement is proportionate in that the information shared will help recover stolen vehicles, protecting the community; deterring criminals who will have reduced income from crime and increasing opportunities for police to catch and prosecute criminals.

Appropriate and necessary in a democratic society:

It is both appropriate and necessary to have such an Information Sharing Agreement in place, as the public would expect the NaVCIS, Tracker and OEMs to cooperate to achieve these goals.

4.2 Schedule 1, Part 2 Data Protection Act (2018)

In order to process and share special category personal data, **at least one Substantial Public Interest Condition must be satisfied.**

Q30. Select the condition(s) that apply from the list below and explain why:

Statutory etc and government purposes Section 6(1)(2).	N
Administration of justice and parliamentary purposes Section 7(a)(b).	N
Preventing or detecting unlawful acts Section 10(1)(2)(3).	N
Protecting the public against dishonesty etc Section 11(1)(2).	N
Regulatory requirements relating to unlawful acts and dishonesty etc Section 12(1)(2).	N
Preventing fraud Section 14(1)(2).	N



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Suspicion of terrorist financing or money laundering Section 15(a)(b). In relation to the 'Purpose' of this agreement	N
Safeguarding of children and of individuals at risk Section 18(1)(2)(3)(4).	N



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

4.3 Schedule 1, Part 3 Data Protection Act (2018)

In order to process and share personal data, **at least one additional condition relating to criminal convictions** in Schedule 1, Part 3 must be satisfied.

Q31. Select the condition(s) that apply from the list below and explain why:	
Consent Section 29.	Y
Protecting individual's vital interests Section 30(a)(b).	Y
Personal data in the public domain Section 32.	N
Legal claims Section 33(a)(b)(c).	N
Judicial acts Section 34.	N
Administration of accounts used in commission of indecency offences involving children Section 35(1)(2)(3)(4).	N
Extension of conditions in Part 2 of this Schedule referring to substantial public interest Section 36.	N



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

4.4. Schedule 8, Part 3, Data Protect Act (2018)

In order to process and share special category data, **at least one condition relating to Special Category Data** in Schedule 8, Part 3 must be satisfied.

Q32. Select the conditions that apply from the list below and explain why:	
Statutory etc purposes Section 1(a)(b).	N
Administration of justice Section 2.	N
Protecting individual's vital interests Section 3.	N
Safeguarding of children and of individuals at risk Section 4(1)(2)(3)(4).	N
Personal data already in the public domain Section 5.	N
Legal claims Section 6(a)(b)(c).	N
Judicial acts Section 7.	N
Preventing fraud Section 8(1)(2).	N
Archiving etc Section 9(a)(b)(c).	N



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

4.5. Data Protection Principles

For additional information about the six Data Protection Principals, please see appendix A.

Article 5 of the GDPR stipulates the key responsibilities for organisations in processing Personal and Special Category Data.

Under the GDPR and Data Protection Act (2018), all individuals have rights concerning how their data is used.

- Signatories to this agreement will respond to any notices from the Information Commissioner that impose requirements to cease or change the way in which data is processed.
- The NaVCIS reserves the right to withdraw the use of this data at any time.

First Principle

The processing of Personal Data for a Law Enforcement Purpose must be lawful and fair.

This ISA will invoke: Common Law in order to share Personal and Special Category data. Data Protection Act 2018, part 3 applies - “The law enforcement purposes”

Q33. Explain why you are using this primary legal gateway and what Acts (including the section and subsection) you are relying on:

The police have a common law duty to prevent and detect crime and a corresponding power to disclose information where necessary for the prevention and detection of crime. In exercising this power they must act fairly, having regard for the circumstances of the case and bearing in mind that such a disclosure is an exception to the general rule of confidentiality. They should also bear in mind that both the public and government expect the police to use their powers and knowledge to prevent crime and to reduce crime and disorder.

Data Protection Act 2018, part 3 applies - **“The law enforcement purposes”**

For the purposes of this Part, “the law enforcement purposes” are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

People should have a legitimate expectation about how their data will be used. Failure to do so, without a lawful basis would be unfair. To help with this, NaVCIS has produced a Privacy Notice. For more information about this, and where exemptions may apply, please contact NaVCIS (intel@navcis.police.uk) or visit our intranet site.

NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICETrackerTM

Official

Q34. State how you will inform data subjects about the use of their data⁴. If it will not be possible in this case then explain why:

In the initial provision of VINs relating to stolen vehicles, it is not possible to obtain consent or inform the data subjects of NaVCIS use of data in this instance; however VINs are not on their own personal data.

Subsequent data sharing will be with the obtained consent of the relevant vehicle owner, or insurer (responsible at that point for the stolen vehicle.)

Location data supplied by OEMs will only be relevant to location the stolen vehicle and only the criminals are at risk of personal data disclosure, which as during the commission of a crime, is not protected in law.

Second Principle

Personal Data collected for a Law Enforcement Purpose must be specified, explicit and legitimate and must not be processed in a manner that is incompatible with the purpose for which it was collected.

Q35. State how this agreement will comply with the Second Data Protection Principal:

The purpose of this Information Sharing Agreement is to allow police held data to be added to by manufacturer held data, to allow location of stolen vehicles

The processes followed ensure the agreement is applied only to confirmed stolen vehicles and that there are regular checks to ensure any vehicles subject to being located, are still stolen and outstanding.

Personal data collected and processed will be for the lawful enforcement purposes stated in this agreement and will not be processed in a manner that is incompatible with the purpose for which it was collected.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

Third Principle

Personal Data processed for a Law Enforcement Purpose must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

Q36. State how this agreement will comply with the Third Data Protection Principal:

As a national police unit, NaVCIS supports and creates opportunities to reduce and disrupt crime and to protect life.

This is in part achieved through the sharing of information with partners and law enforcement agencies.

For many years, Tracker have worked closely with a number of vehicle manufacturers (OEM's) for a number of years, ****S31(1)****

****S31(1)****

- Upon receipt of the daily vehicle theft PNC list from NaVCIS, it is proposed that Tracker share relevant Vehicle Identification Numbers only with a Data Handler partner, who would then share this information with a number of OEM's (provides a list to Tracker those that have agreed to sign up to the scheme).
- An assessment will be carried out to establish if any vehicles listed have a potentially viable telematics system installed, with the capability to provide movement and location data.
- Following this assessment, the Data Handler provides a list to Tracker with vehicles that fit this criterion.
- Tracker will provide this specific list to NaVCIS, who then carry out a check to establish if each vehicle is still outstanding, unrecovered and NaVCIS provide Tracker with basic vehicle details, Crime Reference number and name of the vehicle Insurer.

****S31(1)****

- Should a specific vehicle not have a current Insurance Policy listed on PNC, Tracker would contact NaVCIS in the same way and seek support for the Police to contact the owner for consent to activate.
- Upon receipt of agreement from the Insurer or consent from the vehicle owner, Tracker contacts the Data Handler to facilitate activation of the telematics device. Prior to activation, Tracker will contact the local Police Force to establish that the vehicle is still listed as 'stolen' on PNC and hasn't been recovered.
- Once the telematics device is activated, the Data Handler will share any location of movement data for that vehicle (only whilst the vehicle remains 'outstanding'). This information will be shared with the relevant Police Force in a timely way in support of attempts to locate and recover the stolen vehicle.
- Once the telematics device is activated, Tracker via the Data Handler will stream data for each



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

particular stolen vehicle for a maximum of 30 days (unless specifically requested to extend this time period by Law Enforcement). At every given point throughout this period, Tracker will contact the relevant Police Force upon receipt of location and movement data by way of update and to establish that the vehicle is still 'outstanding', unrecovered.

- Any Data held throughout this process will be stored for a maximum of 365 days (unless a request for any such data to be held for a longer period is specifically required by Law Enforcement). The data will be available to Law Enforcement throughout this period in support of ongoing criminal investigations/Court proceedings etc.).
- During this period of time, the data will be held at Tracker via our Salesforce CRM account. This account is not shared outside the European Economic Area.

Fourth Principle

Personal Data processed for a Law Enforcement Purpose must be accurate and, where necessary, kept up to date.

Q37. State how this agreement will comply with the Fourth Data Protection Principal: Include what measures are in place to ensure the data shared by the NaVCIS and or the Partner Organisation(s) is accurate and up to date and who is responsible for informing the NaVCIS and or the Partner Organisation(s) of inaccuracies or notifications of new information such as a change of address.

This data will be subject to standard NaVCIS procedures and validations to ensure that is accurate and relevant. As Tracker are reliant upon the accuracy of the data supplied by NaVCIS it would be difficult for them to identify any inaccuracies. To circumvent this NaVCIS will quality assure all data it shares with Tracker.

Fifth Principle

Personal Data processed for a Law Enforcement Purpose must be kept for no longer than is necessary for the purpose for which it is processed.

It may be stored for longer periods for research, statistical or archiving purposes in the public interest, subject to the implementation of appropriate measures to safeguard the rights and freedoms of individuals.

Q38. State how this agreement will comply with the Fifth Data Protection Principal: Include a statement about how long the NaVCIS and or the Partner Organisation(s) will keep the data for.

The retention of information, including personal data legitimately obtained and retained will be determined by standard NaVCIS policy and procedure.

The information that is to be supplied to Tracker by NaVCIS shall be kept securely until it is no longer relevant and necessary and for a maximum of 365 days; unless requested by a police force to retain for longer, at which Tracker will follow police retention period.

NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICETrackerTM

Official

Sixth Principle

Personal Data processed for a Law Enforcement Purpose must be so processed in a manner that ensures appropriate security of the Personal Data.

This includes the protection against unauthorised or unlawful processing and against accidental loss, destruction or damage using appropriate technical or organisational measures.

Q39. State how this agreement will comply with the Sixth Data Protection Principal:
Tracker and the parties involved have appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(a) to 32(d) (inclusive) of the GDPR.

4.6. Freedom of Information and Right of Access Requests

FOIA Requests: Normal practice will be to make all DSAs externally available on the NaVCIS Publication Scheme. It is recognised that parties to this agreement may receive a request for information made under FOIA that relates to the operation of this agreement. Where applicable, all Partner Organisation(s) will observe the Code of Practice made under Section 45 of the FOIA, relating to consultation with others who are likely to be affected by the disclosure (or non-disclosure) of the data requested. The Code also relates to the process by which one authority may also transfer all or part of a request to another authority if it relates to data held only by the other authority.

Right of Access Requests (GDPR and DPA 2018): Individuals can request a copy of all the data an organisation holds on them, by making a Right of Access request (ROAR). This may include data that was disclosed to that organisation under this agreement. Where this is the case, as a matter of good practice, the organisation will liaise with the originating agency to ensure that the release of the data to the individual will not prejudice any ongoing investigation/proceedings.

- The Signatories of this agreement will comply with right of access requests in compliance with the relevant legislation (GDPR/DPA 2018), and if it is to be answered jointly, to inform the NaVCIS as soon as possible on receipt in order to comply with the statutory time limit.



NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

TrackerTM

Official

Section 5. Agreement signatures

The Signatory Organisations signing this agreement accept that the procedures laid down in this document provide a secure framework for the sharing of data between their agencies in a manner compliant with their statutory and professional responsibilities.

As such, they undertake to:

- Implement and adhere to the procedures and structures set out in this agreement.
- Accept responsibility to ensure that all staff involved are trained and fully aware of the procedures and structures of the agreement.
- Ensure that where these procedures are complied with, no restriction will be placed on the sharing of data other than those specified within this agreement.
- Engage in a review of this agreement with partners three months after its implementation and annually thereafter.

We the undersigned agree that each Partner Organisation that we represent will adopt and adhere to this Information Sharing Agreement:

Agency	Post Held	Name	Signature	Date
NaVCIS	Head of Unit	**S40(2)**	**S40(2)**	20/07/23
Tracker	Managing Director	Mark Rose	**S40(2)**	November 10,20
High Mobility	Business Development Manager	**S40(2)**	**S40(2)**	November 10,20



Appendix A

Data Protection Principals

First Principal

The processing of personal data for a law enforcement purpose must be lawful and fair.

The ICO website says the following:

You need to be aware that any processing you carry out for the law enforcement purposes must be necessary. In practice, the lawful basis would either be necessary for the performance of a task carried out for law enforcement purposes by a competent authority, or based on consent. There may be circumstances where you obtain consent from the individual whose data you are processing, although this may only be appropriate in certain circumstances. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

- Lawful (processing) - means that you are authorised by either statute, common law or royal prerogative, or by or under any other rule of law.
- Fair - requires you to be, where appropriate, clear and open with individuals about how you use their information, in keeping with their reasonable expectations.

When processing Special Category Data:

You must be able to demonstrate that the processing is **strictly necessary** and satisfies one of the conditions in Schedule 8 or is based on consent. Strictly necessary in this context means that the processing has to relate to a pressing social need, and you cannot reasonably achieve it through less intrusive means. This is a requirement, which will not be met if you can achieve the purpose by some other reasonable means.

Second Principal

Personal data collected for a Law Enforcement purpose must be specified, explicit and legitimate and must not be processed in a manner that is incompatible with the purpose for which it was collected.

The ICO website says the following:

Any processing under Part 3 of the Act must be for the defined law enforcement purposes. You cannot process for a purpose that is incompatible with the original reason and justification for processing.

Third Principal

Personal data collected for a Law Enforcement Purpose must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

The ICO website says the following:

The third principle requires that the personal data you are holding is **adequate** and **limited to** what is necessary for the purpose(s) you are processing it.

NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICETrackerTM

Official

Fourth Principal

Personal data processed for a Law Enforcement Purpose must be accurate and where necessary, kept up to date.

The ICO website says the following:

The fourth data protection principle is about accuracy. It sets out that you should take every reasonable step to correct inaccurate data. In addition, **as far as possible**, you need to be able to distinguish between personal data that is based on factual data and that which is based on a matter of opinion or assessment, such as a witness statement.

A new requirement is that again, where relevant, and as far as possible, you need to be able to distinguish data between different categories of individuals, such as suspects; individuals who have been convicted; victims and witnesses. You only categorise information under Part 3 that is relevant to your investigation, and other unused data falls under the general provisions of GDPR and Part 2 of the Act.

Fifth Principal

Personal data processed for a Law Enforcement Purpose must be kept for no longer than is necessary for the purpose for which it is processed.

The ICO website says the following:

The fifth principle requires that you do not keep personal data for longer than is necessary for the purpose you originally collected it for. No specific time periods are given but you need to conduct regular reviews to ensure that you are not storing for longer than necessary for the law enforcement purposes.

Sixth Principal

Personal data processed for a Law Enforcement Purpose must be so processed in a manner that ensures appropriate security of the personal data.

The ICO website says the following:

The sixth principle requires you to have technical and organisational measures in place to ensure that you protect data with an appropriate level of security. This is the same as under GDPR and Part 2 of the Act.

‘Appropriate security’ includes ‘protection against unauthorised or unlawful processing and against accidental loss, destruction or damage’.

NATIONAL VEHICLE CRIME
INTELLIGENCE SERVICE

Tracker™

Official

Appendix B

Evidence of Consent

Please attach here a copy of the consent form you will use.

NaVCIS receives information, (such as reported stolen vehicles across the UK), from police partners and systems such as the Police National Computer.

NaVCIS provides a regular list of recently stolen vehicles, containing the bare minimal of data, to Tracker Network (UK) Ltd; to allow Tracker to facilitate locating the stolen vehicles through their own location hardware (if present); or using third party hardware/ software systems

****S31(1)****

At the point of sharing the minimal data, it is not practicable to obtain consent from relevant subjects. The data shared cannot in any case be linked to a subject without additional information from a police system – which any party with access to, could achieve without the list from NaVCIS. Therefore the data shared in this agreement is the bar minimum to achieve the stated aims and has no additional data risk to the data subjects.

The ICO guidance and DPA 2018 are clear that lawful exemption from obtaining consent exists for 'The law enforcement purposes' (DPA 2018); the ICO guidance states that where the data would be processed regardless of consent, 'then asking for it is misleading and inherently unfair'.

It is the position of NaVCIS head of Unit, that the above applies and so the consent form is not applicable in these circumstances.