

# Data Sharing Agreement

North Tyneside Council and  
Northumbria Police



North  
Tyneside  
Council

## Contents

|                                                                   |    |
|-------------------------------------------------------------------|----|
| 1. Preamble.....                                                  | 2  |
| 2. Definitions.....                                               | 2  |
| 3. Parties .....                                                  | 2  |
| 4. Term .....                                                     | 3  |
| 5. Purpose (Agreed Purpose) .....                                 | 3  |
| 6. Shared Personal Data .....                                     | 3  |
| 7. Compliance with the Data Protection Legislation .....          | 4  |
| 8. Process.....                                                   | 4  |
| 9. Data Quality.....                                              | 4  |
| 10. Data Subject Rights .....                                     | 4  |
| 11. Data Retention and Disposal .....                             | 5  |
| 12. Transfers .....                                               | 5  |
| 13. Training and Security .....                                   | 5  |
| 14. Data Breaches and Reporting Protocols .....                   | 5  |
| 15. Indemnity .....                                               | 5  |
| 16. Signatories .....                                             | 6  |
| Schedule 1 – Further Detail on Shared Personal Data.....          | 7  |
| Schedule 2 – Single Point of Contact (SPoC) .....                 | 8  |
| Schedule 3 – Data Quality and Compatible Datasets .....           | 9  |
| Schedule 4 – Deletion Procedure.....                              | 10 |
| Schedule 5 – Technical and Organisational Security Measures ..... | 11 |

**Between**  
**North Tyneside Borough Council (the "Authority")**  
**and**  
**Northumbria Police (the "Police")**

**Version 1**

**Effective date: 26 February 2026**

## **1. Preamble**

The purpose of this Agreement is to define how personal data and special category data captured by the Authority's CCTV system will be shared between North Tyneside Borough Council and Northumbria Police. The Authority owns and maintains the corporate CCTV system hosted on the Verkada platform. Northumbria Police will be granted controlled access to live and recorded footage as an independent data controller for legitimate law enforcement purposes.

## **2. Definitions**

- Agreed Purpose: Has the meaning given to it in clause 5 of this Agreement.
- Agreement: This Agreement is a free-standing document that does not incorporate commercial business terms established by the parties under separate arrangements.
- Data Sharing Code: The Information Commissioner's Data Sharing Code of Practice (December 2020).
- Data Protection Legislation: The UK Data Protection Act 2018; the UK GDPR; the Privacy and Electronic Communications Regulations; and other applicable laws and guidance.
- Personal Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Shared Personal Data.
- Shared Personal Data: The personal data and, where applicable, special category personal data to be shared between the parties as detailed in clause 6 and *Schedule 1*.

## **3. Parties**

Data Sharing Agreement for the sharing of data between:

- North Tyneside Borough Council ("**Data Discloser**")

Principal office: Quadrant East, The Silverlink North, Cobalt Business Park, North Tyneside, NE27 0BY

- Northumbria Police ("**Data Receiver**", *Independent Controller*)

Principal office: Northumbria Police Headquarters, Middle Engine Lane, Wallsend, NE28 9NT

#### 4. Term

This Agreement commences on the Effective date above and will be reviewed annually or sooner if legislative, operational or system changes require.

#### 5. Purpose (Agreed Purpose)

This Agreement sets out the framework for sharing CCTV personal data between the parties as independent controllers. It defines the principles and procedures that the parties shall adhere to, and the responsibilities owed to each other.

The Authority operates a network of CCTV cameras on the Verkada system for community safety and the protection of individuals and public spaces. Granting Northumbria Police access to live and historic footage will enhance prevention and detection of crime and anti-social behaviour, support timely searches for vulnerable or missing persons, and secure vital evidential material.

The use of this service will support Northumbria Police to efficiently gather and securely store digital evidence. Allowing officers to quickly obtain this themselves will improve existing processes currently operated within the force.

#### 6. Shared Personal Data

- Personal Data: CCTV images of identifiable individuals; vehicle images; associated metadata including timestamps, camera identifiers and locations; user access logs for auditing.
- Special Category Data (captured incidentally): racial or ethnic origin (as visible), health-related indicators (e.g. visible injuries), biometric data (facial imagery) where used for identification by the Police.
- Criminal offence data: footage relevant to suspected criminal activity, investigations and proceedings.

Further detail is set out in *Schedule 1*, together with any access and processing restrictions agreed by the parties.

## **7. Compliance with the Data Protection Legislation**

Each party shall ensure that it processes the Shared Personal Data fairly and lawfully.

The Authority relies on UK GDPR Article 6(1)(e) (public task) and Article 9(2)(g) (substantial public interest) with DPA 2018 Schedule 1 conditions (preventing/detecting unlawful acts; public protection; safeguarding).

The Police process Shared Personal Data under Part 3 of the Data Protection Act 2018 for law enforcement purposes (prevention, investigation, detection or prosecution of criminal offences).

Each party has a valid registration with the Information Commissioners Office (ICO), if required which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this Agreement.

## **8. Process**

- Access to the Verkada system will be provided through named, authorised accounts issued by the Authority with role-based permissions.
- Two-factor authentication (2FA) will be enforced. All user activity (viewing, searches, exports) is logged and auditable.
- Access is restricted to officers and staff in North Tyneside Area Command across Response, Neighbourhood, CID and specialist units, from Constable to Chief Superintendent.
- Footage may only be used for the Agreed Purpose and must be handled in accordance with force evidence policies.

## **9. Data Quality**

The Authority will take reasonable steps to ensure the accuracy and integrity of CCTV footage. The Police must verify the accuracy and context of any footage before operational use. Any identified inaccuracies will be notified between SPoCs and, where possible, corrected.

## **10. Data Subject Rights**

Each party will provide reasonable assistance to enable the other to respond to requests from data subjects. Given the law-enforcement nature of processing, the Police may apply applicable restrictions under Part 3 DPA 2018 where necessary and proportionate. The Authority will manage initial CCTV requests and liaise with the Police as appropriate.

## **11. Data Retention and Disposal**

The Authority will retain CCTV footage in line with the corporate retention schedule applicable to the Verkada system (typically 28–31 days unless required for an investigation).

Where the Police export or receive footage, it becomes Police-held data and will be retained in accordance with force retention policies (Management of Police Information – MOPI) and evidential requirements and deleted once no longer necessary.

Deletion actions and confirmations will follow the process in *Schedule 4*.

## **12. Transfers**

The Police shall not disclose Shared Personal Data to third parties except where lawful and necessary for law enforcement purposes. No international transfers are envisaged. If a transfer is required, the transferring party will ensure appropriate safeguards are in place in accordance with the Data Protection Legislation.

## **13. Training and Security**

Both parties will maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including access controls, authentication, encryption in transit and at rest (where available), secure storage, and audit logging.

Staff accessing the system will be trained and subject to confidentiality obligations proportionate to their role. The Authority will provide access user guides specific to Verkada controls; the Police will ensure that all users have completed appropriate information security and evidential handling training.

## **14. Data Breaches and Reporting Protocols**

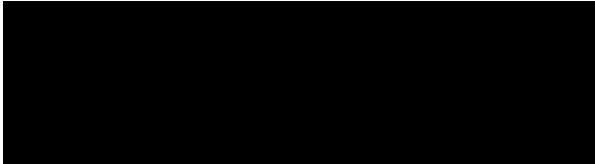
Each party will inform the other without undue delay of any actual or suspected personal data breach involving the Shared Personal Data, and cooperate to investigate and remediate the incident.

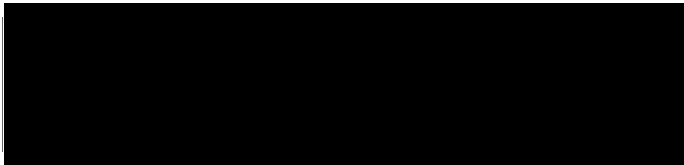
The parties will assess whether notification to the ICO and/or data subjects is required and will support each other in meeting any statutory obligations.

## **15. Indemnity**

Each party undertakes to indemnify the other against direct losses arising from its breach of this Agreement to the extent permitted by law.

**16. Signatories**

|                     |                                                                                    |
|---------------------|------------------------------------------------------------------------------------|
| <b>Organisation</b> | For and on behalf of North Tyneside Borough Council                                |
| <b>Name</b>         |  |
| <b>Signature</b>    |  |

|                     |                                                                                    |
|---------------------|------------------------------------------------------------------------------------|
| <b>Organisation</b> | For and on behalf of Northumbria Police                                            |
| <b>Name</b>         |  |
| <b>Signature</b>    |  |

## **Schedule 1 – Further Detail on Shared Personal Data**

### **Classification: Personal Data**

- CCTV images of identifiable individuals
- Vehicle images and registration plates (where captured by camera capability)
- Timestamps, camera identifiers, locations
- User access and audit logs (for investigation/audit)

### **Classification: Special Category Personal Data (captured incidentally)**

- Racial or ethnic origin (visual inference only)
- Health indicators (e.g., visible injuries)
- Biometric data (facial imagery) for identification by the Police

### **Classification: Personal Data processed for law enforcement purposes**

- Criminal offence data and intelligence indicators within footage
- Evidence for investigation and prosecution

**Schedule 2 – Single Point of Contact (SPoC)**

|                     |                        |
|---------------------|------------------------|
| <b>Organisation</b> | North Tyneside Council |
| <b>Name</b>         | [REDACTED]             |
| <b>Position</b>     | [REDACTED]             |
| <b>Phone Number</b> | [REDACTED]             |
| <b>Email</b>        | [REDACTED]             |

|                     |                                                  |
|---------------------|--------------------------------------------------|
| <b>Organisation</b> | Northumbria Police – North Tyneside Area Command |
| <b>Name</b>         | [REDACTED]                                       |
| <b>Position</b>     | [REDACTED]                                       |
| <b>Phone Number</b> | [REDACTED]                                       |
| <b>Email</b>        | [REDACTED]                                       |

### **Schedule 3 – Data Quality and Compatible Datasets**

CCTV images are captured automatically and can be affected by environmental conditions (lighting, weather, occlusion). Both parties will take reasonable steps to ensure data are accurate and up to date for the Agreed Purpose. The Police will corroborate footage with other evidence where appropriate.

#### **Schedule 4 – Deletion Procedure**

1. Authority: automated deletion in Verkada in accordance with retention schedule unless footage is preserved for an investigation.
2. Authority: where footage is preserved at Police request, the Authority will mark the clip for extended retention or export to a secure channel, recording the request and legal basis.
3. Police: exported footage stored only in accredited force systems; retain in line with MOPI/evidential requirements; delete when no longer necessary; record deletion.
4. Either party: confirm deletion to the other party on request via the SPoCs.

## **Schedule 5 – Technical and Organisational Security Measures**

Law Enforcement Digital Evidence Principles (NPCC/ACPO – summary):

- No action should be taken which changes data held as digital evidence; where access to original data is necessary, the person accessing must be competent and able to explain the relevance and implications.
- An audit trail of all processes applied to digital evidence must be created and preserved; an independent third party should be able to reproduce the same result.
- The officer in charge has overall responsibility to ensure these principles are adhered to.
- Verkada platform: role-based access controls; organisation-wide 2FA enforcement; centralised audit logs; configurable archive permissioning.
- Secure network access via HTTPS/TLS; encryption at rest as provided by the platform; least-privilege roles for Police users; time-bound access where appropriate.
- Export controls: only authorised users may export; exports to be watermarked where available; exports stored in secure Police evidence systems with chain-of-custody records.
- Device and environment security: cameras physically secured; default credentials disabled; firmware kept up-to-date; privacy regions / face blurring configured where appropriate.
- Incident response: suspected misuse or breach to be reported immediately to both parties; logs preserved for investigation.