CLEVELAND POLICE

Community Safety Partnership Analysts Access to Force Systems and Software

Policy Number	198
Policy Owner	Head of Intelligence
Version	4.4
Last Review Date	August 2022
Next Review Date	August 2025
Date of approval	May 2012 for note
Protective Marking	Official

This document has been assessed for:	
Compliance with Legislation	☒
Equality Impact Assessment	☐
Freedom of Information issues	☒
Human Rights compliance	☒
Health and Safety	☒
Risk Management	☒

Community Safety Partnership Analysts Access to Force Systems and Software

1. Policy statement

Cleveland Police will ensure collaborative working with Local Authority analytical staff, particularly those working within the Community Safety Partnerships, by providing access to specified Force systems and software, ensuring compliance with corporate standards for information security.

The procedures set out in this document apply to all Police Officers, Police Staff; including those employed by the Police and Crime Commissioner and partner agencies where appropriate, Special Constables and Volunteers.

This policy must be applied fairly, equally, and consistently by and to all Police Officers and employees irrespective of age, disability, gender reassignment, marriage or civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation or any other unjustifiable grounds.

2. Purpose

This policy aims to provide a corporate and consistent approach to assessing and authorising access to specified Force systems and software for partnership analytical staff, considering two levels of access- general and enhanced. This policy will define a set of standards and requirements that must be met to gain access to Force systems and software. A signed Memorandum of Understanding (MOU) will underpin each successful application, as detailed in Appendix 1.

This document supports the force's policing priorities:

- Serving the public and putting communities at the heart of all we do;
- Recognising and safeguarding vulnerable victims;
- Preventing crime and anti-social behaviour and tackling criminality;
- Caring for and supporting our people.

3. Underpinning procedures

3.1 Application

This policy applies to all Local Authority analytical staff, particularly those working for the Community Safety Partnerships, requesting access to Force systems.

Each applicant must complete a general level request form, to be endorsed by the applicant's line manager. The form will then be forwarded to the Analysis

Manager and Information Security Officer for review and comment, prior to consideration for authorisation by the Head Intelligence.

The applicant must include the key responsibilities and duties of their post and demonstrate that they require access to Force systems and software to enable them to carry out analysis to support partnership activity. For example, the applicant requires access to:

- Undertake strategic analysis to support production of the CSP strategic assessment or other strategic products / reports;
- Undertake problem solving analysis based on location or theme to support CSP or multi-agency activity;
- Undertake analysis to support tackling neighbourhood priorities through Joint Action Group (JAG) activity.

This must include a description of the research, analytical or intelligence products and reports the applicant intends to produce using data and information obtained from Force systems using analytical software and to whom these products are likely to be disseminated.

3.2 General level of access

General level of access is defined as:

- Access to the Force network with a personal drive and Outlook account;
- Access to the Force intranet;
- Access (read only) to the server Partnership on the O drive (Analytical function – partnership);
- Access (read only) to the SOLAR2 data warehouse (details of the data available is included in Appendix 1);
- Access to Link Explorer analytical software through a network dongle configuration, with access (read only) to locally managed template workfiles;
- Access (read only) to Force base maps and the Link Explorer bridge to allow data to be translated to locally purchased MapInfo Professional mapping software;
- Access to Force Excel analysis tools.

In order to receive the defined general level of access, the standards of information security outlined in the Memorandum of Understanding (MOU) must be implemented. These include:

- Access to the Force systems and software will be from a suitably secure environment (assessed by the Information Security Officer) using a designated desktop PC, located in a Force building;
- The applicant must be vetted to the appropriate level prior to receiving access;

- The applicant must sign the Official Secrets Act declaration and the joint Data Protection and Information Security declaration prior to receiving access;
- The applicant will undertake appropriate training before receiving access and be provided with an induction to information security by the Information Security Officer;
- All work undertaken using Force systems and software will be for the purposes outlined in the application, and the applicant is expected to act in a responsible manner at all times. Unauthorised use of the Force desktop computer, Force computer systems or misuse of the Outlook system may be treated as a potential disciplinary matter.

Partnership Analytical staff will be subject to regular audits in relation to use of Force systems and software and information they have accessed in the course of their work.

A designated Senior Analyst based at Cleveland Community Safety Hub will oversee the applicant's use of Force systems and software. This will:

- Ensure appropriate support and guidance is given to partnership analytical staff;
- Ensure data and information is appropriately referenced and correctly interpreted;
- Prevent duplication of work undertaken by both police and partnership analytical staff;
- Ensure appropriate dissemination of reports and products.

The applicant will therefore:

- Provide the Senior Analyst with access to their Cleveland Outlook account;
- Provide a copy of all research, analytical and intelligence products prepared using Force systems and software to the Senior Analyst by uploading these documents into the analytical function – partnership folder. A selection of these products will be regularly quality assured by the Senior Analyst;
- Attend regular review meetings with the Senior Analyst to discuss work produced using Force systems and software.

3.3 Enhanced level of access

There may be occasions where an enhanced level of access is required for Local Authority, particularly Community Safety Partnership, analytical staff. This may be a requirement of their specific roles and responsibilities or to enable particular pieces of work to be completed.

Enhanced level of access is defined as access to any data or information not provided through general level access, as described above. Applications for this level of access will require completion of an enhanced access request form, to be forwarded to the Analysis Manager and Information Security Officer for consideration, prior to submission to the Head of Intelligence. This will include

assessment of the most appropriate method of providing the required information to the applicant.

3.4 Restrictions

This policy only considers those staff working in analytical roles within the Local Authority either currently working within the Community Safety Partnerships (CSPs) or responsible for work which support the CSPs, such as JAG papers.

4. Appendices

Appendix	Description
1.	Data available within the SOLAR 2 data warehouse
2.	Memorandum of Understanding
3.	Request form – general level for CSP analytical staff
4.	Request form – enhanced level for CSP analytical staff

5. Compliance and monitoring

The Head of Intelligence is responsible for the accuracy and integrity of this document. This policy will be continuously monitored, and updated when appropriate, to ensure full compliance with legislation.

The Head of Intelligence will review this process to ensure that all aspects are being adhered to in accordance with the framework of this policy.

6. Version control

This policy will be reviewed and updated at least every three years by the owner, and more frequently if necessary.

The Corporate Services Department will ensure this document is available on the Force intranet, including any interim updates.

The following identifies all version changes.

0.1	Jan 2010	New Policy	[redacted]
1.0	May 2010	Policy approved at SDG	[redacted]
1.1	May 2012	Policy review	[redacted]

2.0	May 2012	Approved at SDG	[redacted]
2.1	Nov 2012	Policy amended to reflect introduction of PCC, statement only	[redacted]
3.0	Sep 2013	Policy reviewed and amended to reflect changes as a result of implementation of the Tasking, Co-ordination and Performance Command	[redacted]
4.0	Apr 2016	Policy reviewed and amended to reflect changes as a result of managerial changes within the Force Tasking and Coordination and Operations Command	[redacted]
4.1	Sept 2017	Change of owner department	[redacted]
4.2	Jan 2018	Policy reviewed, no changes required.	[redacted]
4.3	May 2020	Policy reviewed and amended to reflect changes as a result of restructure changes within the Force Intelligence Function. Policy also amended to reflect slight changes in partnership analytical service provision in the different local authorities (all four LPAs do not have dedicated CSP analysts). Name changed to reflect focus of policy.	[redacted]
4.4	August 2022	Policy reviewed, no changes required. Re-formatted to current standard.	[redacted]

Appendix 1:

Data available within the SOLAR2 data warehouse via Link Explorer (also known as Watson) analytical software:

- Crime records including linked-
    - Location
    - Vehicle
    - Person (suspect and / or victim)
    - Stolen property
- Incident records including linked-
    - Location
    - Vehicle
    - Person
- Custody records

APPENDIX 2
MEMORANDUM OF UNDERSTANDING

1. This Memorandum of Understanding is dated ( ), and is entered into by:

   (i) Name of the organisation / partner;
   (ii) The Head of Intelligence (hereinafter referred to as 'Cleveland Police');
   (iii) (Title and Name of the individual involved, and from which organisation) hereinafter referred to as (Title).

2. (i) The parties agree that providing access to Force systems and software will enhance the performance of (Title), whose role and duties are detailed in the request submitted.

   (ii) On a day to day basis the (Title) will be supervised and guided in their work by their own supervisor ( ). Any analytical products created by the (Title) using Force systems and software and / or incorporating Force data must be compliant with the standards set by Cleveland Police in cognisance of guidance issued by the College of Policing (including practice advice on the National Intelligence Model and analytical techniques and products). A designated Senior Analyst within the Force Analytical Function team will be responsible for overseeing the work conducted by the (Title) using Force systems and software and ensure that products are disseminated appropriately (outlined in the supporting policy).

   (iii) The assessment and monitoring of performance will be undertaken by the (supervisor's details). Any issues in relation to performance are to be discussed with the designated Senior Analyst and / or Analysis Manager and reported to the Information Security Officer. At the request of (Organisation) a written or verbal report will be provided in relation to the designated Senior Analyst's observation of the performance of the (Title).

3. (i) Before taking up the position the (Title) must be vetted, this will be undertaken by the Force Vetting Unit.

   (ii) The (Title) must sign the Official Secrets Act Declaration and the joint Data Protection and Information Security Declaration. This document will be retained by the Information Security Officer.

   (iv) Cleveland Police will allocate to the (Title) suitable accommodation within the Force estate. The accommodation will be furnished and will include the provision of a telephone and a networked computer with appropriate software as described in the policy however the computer will be funded through (name of organisation or initiative) and purchased via the Force Procurement system and badged by ICT.

Authorisation from each system owner will be obtained and all training undertaken before access to the Force systems and software is permitted.

The (Title) will be recorded on the Force Human Resource system and will be allocated a Cleveland Police ID.

All work undertaken on the Force desktop computer must be in pursuance of the role of the (Title). Unauthorised use of the Force desktop computer, Force computer systems or misuse of the email system may be treated as a potential disciplinary matter. Access to the Force network and information systems will be suspended immediately. The (Title) is expected to use the Force desktop computer, the computer applications and the internal and external email in a responsible manner and abide by the Cleveland Police policies that are in force. (Title) will be subject to regular audits in relation to use of Force systems and software and information they have accessed in the course of their work.

Cleveland Police reserve the right to access the computer, software, hardware and email facilities without further authority to ensure compliance with security and the requirements for appropriate use. In this respect the (Title) will provide access to their Outlook account to the designated Senior Analyst who will carry out regular audits of emails received and sent.

The (Title) will ensure that a password protected screen saver will be utilised on the Force desktop computer; in addition the time lockout facility will be utilised when not at the desk. The (Title) will not use any other Force desktop PC or laptop other than those that have been designated for the individual's use by the Head of Intelligence.

(iv) The Information Security Officer will provide the (Title) with an induction to information security. This will be arranged by the designated Senior Analyst in liaison with the Information Security Officer.

(v) Cleveland Police and the office of the Police and Crime Commissioner will maintain a policy of insurance providing Public Liability Insurance with a limit of £25m per claim.

(vi) The (Title) will have access to the designated Local Policing Area police station during working hours only and will only enter areas specific to their role. The (Title) will have access to appropriate rest facilities. The (Title) will comply with any security measures identified by the Local Policing Command; failure to comply with such measures will result in access to the police station being withdrawn and consideration given to disciplinary proceedings.

(vii) The (Title)'s access to Local Policing Area police station will be via the station front door. The (Title) will not be issued with a box key but where

appropriate will be issued with an access card where secure access is in place.

(viii) The (Title) will wear their identification pass from the (Organisation) at all times whilst in a police building.

(ix) The (Title) acknowledges that they are working within an operational police station and the demands of police operations may, from time to time, place further restrictions on their movement within the police station. Such further restrictions will be made known to them and the (Organisation) in writing by the Local Policing Command.

(viii) The (Title) must treat all information obtained from Force systems and software in the strictest confidence. Inappropriate and unjustified disclosure of any information will be viewed in the most serious manner by Cleveland Police and (Organisation) and may result in:

a. Exclusion from the police station.
b. Disciplinary action by (Organisation) of which dismissal is an option following appropriate investigation.
c. Criminal proceedings.

The (Title) will comply with the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act and all Cleveland Police Information Security Policies in force.

All printing/copying of police documents must be controlled and monitored and no Force document, printout or electronically held data to be removed from ( ) police station unless this has been authorised by the designated Senior Analyst.

(ix) Cleveland Police may refer any matter of concern regarding the (Title) to the (Organisation) for action as the (Organisation) sees fit. Cleveland Police may require the (Title) to vacate the premises of ( ) police station, but will give the (Organisation) one month's notice of the date by which the premises must be vacated, except in wholly exceptional circumstances when the (Title) may be required to vacate the premises immediately.

(x) It is recognised that, from time to time, matters will arise beyond the scope of this formal Memorandum. Such matters will be discussed by the (Organisation), Cleveland Police and the (Title), with a view to reaching agreement about any such matter. It is recognised that there is no intention to create any legal liability in relation to the occupation of office space by the (Title).

(xi) This initiative will be in place for (duration if known).

(xii) If identified that a deputy needs to be in place to cover for periods of absence then the named individual must undergo the same procedure as detailed in this Memorandum of Understanding.

Signed by the parties as follows:

1. On behalf of the (Organisation)

.....
(Title)

2. On behalf of Cleveland Police

.....
(Head of Intelligence)

.....
(Supt, Local Policing North and/or South, Local Policing Command)

3. (Title) of the (Organisation)

.....

Dated: _____

CLEVELAND POLICE

Request form for GENERAL LEVEL access to Force systems and software by Local Authority/Community Safety Partnership (CSP) analytical staff

APPLICANT DETAILS	
Name of requesting Local Authority/CSPAnalyst:	
Role title:	
Local authority:	
Contact telephone number:	

BUSINESS CASE
Please outline the key duties and responsibilities of your post, demonstrating why you require general level access to Force systems and software, referring to the requirements outlined in the Force policy. This must include a description of the research, analytical or intelligence products and reports the applicant intends to produce using data and information obtained from Force systems using analytical software. Please expand onto a second page if required.

ENDORSEMENT BY CSP LINE MANAGER / SUPERVISOR	
Name:	
Date:	
Contact telephone number:	

ENDORSEMENT BY SUPT FOR NORTH OR SOUTH, LOCAL POLICING COMMAND	
Name:	
Date:	
Contact telephone number:	

Please forward the completed request form with appropriate endorsement to the Analysis Manager, Force Intelligence.

REVIEW BY ANALYSIS MANAGER	
Name:	
Date:	
Comments:	

REVIEW BY INFORMATION SECURITY OFFICER	
Name:	
Date:	
Comments:	

REVIEW BY HEAD OF INTELLIGENCE	
Name:	
Date:	
Comments:	

CLEVELAND
POLICE

**Request form for ENHANCED LEVEL access
to Force systems and software by
Local Authority/Community Safety Partnership (CSP) analytical staff**

APPLICANT DETAILS	
Name of requesting Local Authority/CSPAnalyst:	
Role title:	
Local authority:	
Contact telephone number:	

BUSINESS CASE
Please outline the key duties and responsibilities of your post, demonstrating why you require enhanced level access to Force systems and software, referring to the requirements outlined in the Force policy. This must include a description of the research, analytical or intelligence products and reports the applicant intends to produce using data and information obtained from Force systems using analytical software. Please expand onto a second page if required.

ENDORSEMENT BY CSP LINE MANAGER / SUPERVISOR	
Name:	
Date:	
Contact telephone number:	

ENDORSEMENT BY SUPT NORTH OR SOUTH, LOCAL POLICING COMMAND	
Name:	
Date:	
Contact telephone number:	

Please forward the completed request form with appropriate endorsement to the Analysis Manager, Force Intelligence.

REVIEW BY ANALYSIS MANAGER	
Name:	
Date:	
Comments:	

REVIEW BY INFORMATION SECURITY OFFICER	
Name:	
Date:	
Comments:	

REVIEW BY HEAD OF INTELLIGENCE	
Name:	
Date:	
Comments:	