



1. RULES & PROTOCOLS

This document, the *Rules & Protocols of Warwickshire Retail Crime Initiative* describes the obligations of Members of the Scheme.

Before becoming a Member of the Scheme, and before accessing any Scheme data, all prospective Members must certify that they have read, understood, and agreed to abide by this document. Access to the Scheme's data will not be given to any Member who does not first certify that they have read, understood, and agreed to abide by this document.

This document is always available to view or download from the Scheme's Disc system.

Contents of this document

1. Name, address and contact information for the Scheme
2. Criteria of Membership
3. Scheme Area
4. The Scheme's Members-only Website
5. Member's obligations under current Data Protection law
6. Participation in the Scheme's Members-only Website
7. General Description of Technical & Organisational Security Measures for Personal Data
8. The Scheme
9. Exclusion Scheme
10. Irrevocable Erasure of Personal Data
11. Sharing Personal Data
12. Ownership and rights of use of images
13. Data Subject Access Requests
14. Other obligations

1. Name, address and contact information of the Scheme:

Warwickshire Retail Crime Initiative, Safer Neighbourhood Team, Rugby Police Station, Newbold Road, Rugby, Warwickshire CV21 2DH Email: enquiries@wrci.org.uk

2. Criteria of Membership

Membership of the Scheme is restricted to:

- a. Owners, or their representatives, of private property or other private facilities open to the public in the Scheme Area (see below)
- b. Officers of public agencies statutorily tasked with the prevention and / or detection and / or reduction of crime and / or anti-social behaviour in the Scheme Area (see Scheme Area below)
- c. Administrators or Sub-Administrators of Partner schemes who share a similar legitimate interest.



3. Scheme Area

The Scheme Area is the county of Warwickshire.

4. The Scheme's Members-only Website and App (*'the Scheme's Disc system'*):

- a. The Scheme's Website (the Disc Desktop) web-address is: <https://www.disc-net.org/wrci>
- b. The Scheme's App (the Disc App) can be downloaded from the AppStore and Google Play Store etc.
- c. Only Members who have been sent a Welcome email from the Scheme and have completed the certification process which is accessed through the Welcome email can access the scheme's Disc system, and the data which is there.
- d. The Scheme's Website is: <https://www.wrci.org.uk>

5. Members obligations under current Data Protection law

The Scheme captures, processes and shares amongst its Members 'Personal Data' relating to persons reported to the Scheme. Use of this data is carefully regulated by current data protection law. To ensure compliance with the law, Members are obliged:

- a. To keep all information received through the Scheme confidential and not to disclose it to any third party, either directly or indirectly, unless required to do so by law or by the order or ruling of a Court or Tribunal or regulatory body.
- b. Not to print any Personal Data from the Scheme's Disc system.
- c. Not to copy any Personal Data from the Scheme's Disc system into any other system.
- d. To submit Incident Reports on persons by using the secure online facilities available through the Scheme's Disc system.
- e. To ensure that information on the Scheme's Disc system is only accessed by or disclosed to other Members of the Scheme.
- f. To ensure that appropriate security measures are employed to prevent unauthorised access to, or alteration, disclosure or destruction of Personal Data provided through the Scheme's Disc system.
- g. To allow the Scheme to audit each Member's compliance with the above obligations.
- h. To ensure that, where relevant, the Member's employer organisation is compliant with current data protection law.

6. Members' participation in the Scheme's Disc system

When a Member observes a person in an act which represents a threat to the Member's premises, property, staff or customers, the Member agrees to submit an Incident Report through the Scheme's Disc system about the event as follows:

- a. Where the person is displayed on the Scheme's Disc system, to make Incident Reports by clicking or tapping on that person's facial image or name as displayed in the Disc system.
- b. Where the person is not displayed on the Disc system, to use the appropriate Incident Report form on the Disc system to submit as much personal information about the person as may be required by other Members to identify the person, and to indicate on the Incident Report if the person is known to the Member.



7. General Description of Technical & Organisational Security Measures for Personal Data

- a. **Technical security:** All personal data will be processed within the Disc system; the security provisions of the Disc systems are described in the document *Littoralis & Disc Data Security & Protection Provisions*; Members can access the Scheme's data only through the Disc Desktop and/or Disc App.
- b. **Organisational security:** Where it is necessary for personal data to be stored temporarily outside the Disc system, the Scheme will do so, where possible, in an encrypted format and/or in a password-protected manner. Where this is not possible, for example where data is held in hard-copy (paper-based), all such data must be secured in a locked cabinet and access will be through the Scheme administrator or a duly authorised deputy or a member of the Board of Management.
- c. Personal Data will be permanently erased (digital) or destroyed (e.g., paper-based) in compliance with the Retention & Erasure policy defined in the Scheme's relevant Privacy Notice(s).

8. The Scheme

a. Targeted Persons

The Scheme may display names and/or images of 'Targeted Persons' on the Scheme's Disc system. These persons have either been subject to a single Incident Report for criminal or anti-social behaviour by Members or their personal information has been supplied to the Scheme by an authorised Partner (e.g., police) for sharing with Members. These persons are not excluded from Members premises.

The purpose of displaying Targeted Persons on the Scheme Website is to:

- i. ensure that such persons are aware that the Scheme knows their identity, and thus to encourage them to desist in any further criminal or anti-social behavior in the Scheme Area.
- ii. enable Members to be aware of, and easily identify, persons who are or have been recently active in low-level crime and/or anti-social behaviour and, where necessary, submit Incident Report(s) about relevant behaviour.

Unless a Targeted Person becomes subject to an Exclusion Notice (*see below*) his/her Personal Data will be withdrawn from display on the Scheme Disc system after 12 months. This data will continue to be accessible in the Disc database only to the Scheme's Administrator and nominated Members with full Administrator rights subject to the Scheme's policy on Irrevocable Erasure of Personal Data (*see below*)

b. Unidentified Persons [ID Sought]

The scheme may display images on galleries for 9 months of unidentified person [ID Sought] who have committed crime and/or anti-social behaviour against a members' business.

If identified, that subject will be removed from the unidentified gallery treated as a potential Target Person. If they do not fit that criteria, they will no longer be shared with Members.

9. Exclusion Scheme

The Scheme may maintain one or more lists or galleries of Excluded Persons.



a. Day-time Excluded Persons

- i. If a person has been subject to an Incident Report relating to retail-related crime and/or anti-social behavior the Scheme will serve an Exclusion Notice on this person, thus designating him/her as an Excluded Person who is excluded from the premises of all Members of the Day-time Scheme.
- ii. The length of exclusion varies from 6 - 24 months and will become effective from the date of the latest relevant incident reported.
- iii. An initial exclusion will be 6 - 12 months but can be 24 months if the person is a cross border offender, the offence is aggravated, examples being de-tagging, foil lined bags and violence, abuse or anti-social behaviour at the time of the offence to shop staff, store detectives the public or any uniformed service.
- iv. If an Excluded Person is subject to an Incident Report submitted by a Member during the period of his/her exclusion, that period of exclusion is extended by 24 months from the date of the latest incident reported.
- v. As soon as an Excluded Person completes his/her period of exclusion, all Personal Data will be removed from the Disc system. If the Administrator believes there is justification for retaining it as a Targeted Person (see 'Targeted Persons' above) his/her information will be managed accordingly and the Data Controller must record a rationale for this extension and note it on the Targeted Person's file in Disc.

b. Night-time Excluded Persons

- i. If a person has been subject to an Incident Report related to night-time related crime and/or anti-social behavior submitted by any Member, the Scheme via Pub Watch meeting will determine if they should be excluded and if agree an Exclusion Notice will be served on this person thus designating him/her as an Excluded Person who is excluded from the premises of all Members of the Night-time Scheme.
- ii. The length of exclusion is 12 - 24 months and will become effective from the date of the latest relevant incident reported.
- iii. If an Excluded Person is subject to an Incident Report submitted by a Member during the period of his/her exclusion, that period of exclusion is extended by 12 - 24 months from the date of the latest incident reported.
- iv. As soon as an Excluded Person completes his/her period of exclusion, all Personal Data will be removed from the Disc system. If the Administrator believes there is justification for retaining it as a Targeted Person (see 'Targeted Persons' above) his/her information will be managed accordingly and the Data Controller must record a rationale for this extension and note it on the Targeted Person's file in Disc.



- v. Unless an Excluded Person becomes subject to a further exclusion period (*see above*) his/her Personal Data will be withdrawn from display on the Scheme Disc system (i.e. will no longer be shared with the Scheme's Members) after 12 months.
- vi. This person's data will continue to be accessible in the Disc database only to the Scheme's Administrator and nominated Members with full Administrator rights in accordance with the Scheme's policy on irrevocable deletion of Personal Data (*see below*)
- vii. In the event of an incidence of serious disorder, the WRCI Administrator may serve an emergency interim exclusion for a period of up to three months at their discretion in order to prevent any potential further incidents. This exclusion must be confirmed at the next scheme meeting. Photographs may be issued in the case of an emergency interim exclusion subject to relevant protocols and Information Sharing Agreements if necessary and in order to prevent further crime and disorder.
- viii. Exclusions will be served via the WRCI Administrator by one of the following means:
 - In person
 - By recorded delivery
 - By posting or delivering to the last known place of abode
 - Envelopes will be marked "private and confidential"

10. Irrevocable deletion of Personal Data

- a. All Personal Data pertaining to any person will be irrevocably deleted from the Scheme's database 12 months after either the last expiry date of any applicable exclusion scheme or the last incident reported relating to the said person, whichever is the latest. Until that time, this data will continue to be accessible only to the Scheme's Administrator and nominated Members with full Administrator rights.
- b. Relevant anonymized (previously Personal) Data will be retained only for historical statistical analysis.

11. Sharing Personal Data

The Scheme may share Personal Data of a person only:

- a. where the receiving Scheme complies with Good Practice to a level comparable with that defined in this document.
- b. where the receiving Scheme shares the same or similar Common Purpose as the Scheme.
- c. where Personal Data to be shared is not subject to restrictions of use which preclude such sharing.
- d. where the receiving Scheme notes and retains a rationale justifying the acquisition of the Personal Data (for example, that the person is likely to travel to the receiving Scheme area).

Subject to agreement of the Board of Management of the Scheme, the Scheme may share Personal Data stored in its database with suitably authorised third-party organisations such as police, other Scheme Administrators etc.

Where Members wish to share data with the Scheme subject to additional conditions they may draw up additional Information Sharing Agreements with the Scheme's Board of Management



12. Ownership and rights of use of images

When a Member submits an image of a person to the Scheme either through the Disc system or through any other method, the Member grants the Scheme full use of the image in accordance with this document, confirms that the image has been obtained in compliance with current Data Protection law and the CCTV Code of Practice, and where relevant asserts his/her ownership of the image, and right to grant usage of it by the Scheme.

In the case of unidentified images of persons, the submitting Member grants the Scheme unlimited rights to share the image with other Schemes and authorised third parties for identifying the person displayed.

13. Data Subject Access Requests

Persons may request access to all and any of their person data processed by the Scheme by means of a Data Subject Access Request and require correction of any data that the persons can show to be incorrect; information on how to submit Subject Access Requests is included in the Scheme's Privacy Notice which is provided to all persons where possible or, only where not possible, made as widely accessible and available as possible to them.

14. Appeals against Exclusion Notices

An Excluded Person may appeal against his/her exclusion. Appeals must be made in writing to the postal address of the Warwickshire Retail Crime Initiative, Safer Neighbourhood Team, Rugby Police Station, Newbold Road, Rugby, Warwickshire CV21 2D, within 14 days of service of the notice stating the grounds for appeal.

- a. On receipt of an appeal any images will be removed from the secure online system pending the finalisation of the appeals process.
- b. Appeals will be read out by the WRCI Administrator and will be heard in the first instance by those present at the next Pub Watch scheme meeting following receipt of the notice of appeal. The members, after discussion, have the right to dismiss the appeal, or remove or reduce the period of exclusion. Each member will have one vote. The decision will be by majority vote. This must be recorded in the minutes of the scheme meeting.

15. Other obligations

In addition to the above obligations, Members are obliged to:

- a. Maintain their contact information on the Scheme's Disc system and ensure that it is correct.
- b. Refer any formal complaint by a person displayed on the Disc system regarding any element in the Disc system or administrative processes or procedures to the Scheme Administrator via the Disc system.
- c. Be aware that all data accessible on the Scheme Disc system is the property of the Scheme except where otherwise stated.