



CODE OF PRACTICE

**For Registered Persons and other recipients of
Disclosure Information**

May 2018

Contents

Introduction to the Code of Practice

Who does this code apply to?	Page 3
Disclosure Offences	Page 4
What happens if the Code is breached?	Page 5

Registered Body Obligations

Registration details	Page 7
Application process	Page 7
Verification of identity	Page 8
Data handling	Page 9
Suitability policy	Page 10
Payment of fees	Page 11
Eligibility	Page 12
Compliance requests	Page 13

Annex

Data Protection Act 2018	Page 15
--------------------------	---------

Introduction to Code of Practice

AccessNI (ANI) was established in April 2008 to provide criminal record certificates. There are specific legal requirements around the provision of such certificates set out in Part V of the Police Act 1997¹. Section 122 of that Act² requires the Minister of Justice to publish a Code of Practice in connection with the use of information provided to, or the discharge of any function by Registered Bodies.

Who does this code apply to?

The Code of Practice applies to all organisations registered with ANI under section 120 of the Police Act 1997³. These are known as Registered Bodies. This includes those Registered Bodies that provide an umbrella function to non-registered organisations. The Code covers any information provided by ANI and made available to the Registered Body by ANI or an applicant.

ANI will seek to ensure compliance with the Code through a full range of assurance management processes, including scheduled visits to the premises where Registered Bodies discharge their functions.

NB: All applicants for an ANI check should be made aware of this Code of Practice and provided with a copy on request.

¹ <http://www.legislation.gov.uk/ukpga/1997/50/part/V>

² <http://www.legislation.gov.uk/ukpga/1997/50/section/122>

³ <http://www.legislation.gov.uk/ukpga/1997/50/section/120>

The Code of Practice does not apply to other third parties.

Disclosure Offences: Sections 123 and 124 of the Police Act 1997⁴

Although disclosure certificates are provided directly to the applicant, Registered Bodies have access to personal information about applicants in the following circumstances;

- in respect of applications submitted for countersigning;
- where certificates are provided to them by their employees or applicants for posts, including volunteers; or
- from the case tracking system provided by ANI.

Recipients of disclosure information through the applicant's copy of the disclosure certificate must note that it is an offence;

- to disclose information contained within an ANI certificate to any person who is not a member, officer or employee of the Registered Body or their client where the Registered Body provides an umbrella function, unless a relevant legal exception applies;
- to any member, officer or employee where it is not related to that employee's duties.

The only exceptions to this are where;

⁴ <http://www.legislation.gov.uk/ukpga/1997/50/section/123>
<http://www.legislation.gov.uk/ukpga/1997/50/section/124>

- the Registered Body has the written consent of the applicant;
- the information is provided to a Government Department;
- the information is provided to any person who has specific legislative powers that enable them to see or obtain such information; or
- the information is provided to a person to whom the Registered Body or their client has a statutory obligation to provide such information.

It is also an offence to;

- Knowingly make a false statement for the purpose of obtaining, or enabling another person to obtain, a certificate.

An offence may also occur where information provided through the case tracking system is used inappropriately.

Registered Bodies believed to have committed an offence will be liable to prosecution, suspension or de-registration.

What happens if the Code is breached?

The Police Act 1997 (Criminal Records) (Registration) Regulations 2007, as amended, set out Conditions of Registration (Regulation 7)⁵. Regulation 7(h) requires Registered Bodies to comply with this Code of Practice.

Failure to comply with Conditions of Registration can result in refusal by ANI to issue disclosure certificates, the suspension and/or cancellation of

⁵ <http://www.legislation.gov.uk/ukxi/2007/3283/regulation/7/made>

registration. Failure to comply with requirements set out in the Data Protection Act 2018 may also result in enforcement action from the Information Commissioner's Office (ICO).

Registered Bodies must report promptly to ANI any suspected malpractice in relation to this code or any suspected offences in relation to the misuse of disclosure certificates.

Registered Body Obligations

The Police Act 1997 (Criminal Records) (Registration) Regulations 2007 set out the obligations a Registered Body must meet in order to retain its registration.

Registration details

ANI maintains a register of all persons and organisations who wish to ask the exempted question under the Rehabilitation of Offenders (Exceptions) Order (Northern Ireland) 1979⁶ and countersign applications for disclosure certificates. Registered Bodies must:

- Keep ANI informed of changes to signatories and organisational changes such as name, address, contact details etc;
- Maintain accounts online, through the NIDirect system and delete either the Registered Body's account or that of individual lead signatory or counter signatories when no longer required;

Application process

Registered Bodies must:

⁶ Please note there is no consolidated version of this legislation available

- Submit applications for an ANI certificate in the format determined by ANI.
- Ensure that applications for ANI certificates are completed accurately and that all data fields determined by ANI as mandatory are completed in full.
- Ensure that any applications submitted electronically are made on the NIDirect system.
- Ensure that log-in and password details for the NIDirect system, provided by ANI, are not shared with anyone that is not a countersignatory. Where details are shared this must be solely for the purpose of countersigning applications.

Verification of Identity

Registered Bodies must:

- Verify the identity of the applicant prior to the submission of an application for an ANI certificate by following the current guidelines issued by ANI.
- Ensure that any person undertaking identity verification checks on their behalf follows the current guidelines issued by ANI.
- Make sure lead or counter signatories do not validate or countersign their own applications for any ANI certificate.

Data Handling

In line with the Data Protection Act 2018, Registered Bodies must:

- Handle all information provided to them by ANI, as a consequence of applying for an ANI certificate, in line with the obligations under Data Protection Act 2018. The principles of the Data Protection Act 2018 are set out at Annex A.
- Handle all information provided to them by their employee or potential employee for an ANI application in line with the obligations under Data Protection Act 2018.
- Ensure that where a certificate or a copy of a certificate is obtained from an applicant that it is not retained longer than is required for the specific purpose of taking a decision on that applicant's suitability. (Please note that information disclosed on AccessNI certificates is regarded under the Data Protection Act as "sensitive personal data" in that it consists of information as to the commission or alleged commission of any offence.)
- Ensure that a result received as part of an application submitted electronically is not reproduced in such a way that it infers that it is a certificate issued by ANI.
- Those bodies providing an umbrella function must ensure that any third parties they deal with in respect of disclosures are aware of the Data Protection Act 2018 and provide them with guidance on secure

handling and storage of information. For Data Protection purposes, information passed to a Registered Body by ANI remains the responsibility of the Registered Body even if passed to a third party.

- Ensure business continuity and disaster recovery measures are in place and comply with Data Protection requirements.
- Must, in particular, comply with security requirements of the Data Protection Act 2018.

AccessNI also requires registered bodies to have a written policy on the secure handling of information provided by ANI and make it available to individuals at the point of requesting the person to complete an ANI application form.

Where ANI considers that a Registered Body may be in breach of the obligations set out in this section, it may report this to the Information Commissioner's Office (ICO). Failure to comply with DPA requirements could result in enforcement action from the ICO.

Suitability Policy

Registered Bodies must:

- Have a written policy on the suitability of ex-offenders for employment in relevant positions that should not unfairly discriminate on the basis of conviction or other information disclosed. This policy should be available upon request to potential applicants and, in the case of those carrying out an umbrella function, should be made available to their clients.

- Ensure that all applicants for relevant positions or employment are notified in advance of the requirement for a criminal record check through ANI.
- Notify all potential applicants of the possible effect of a criminal record history on the recruitment and selection process and any recruitment decision.
- Discuss the content of the Disclosure with the applicant before withdrawing any offer of employment.

Payment of Fees

Registered Bodies must:

- Pay all registration fees in line with time periods set out in Regulations 7(a), (b) and (c) of the Police Act 1997 (Criminal Records) (Registration) Regulations (Northern Ireland) 2007.
- Pay all fees related to criminal records check applications submitted after any decision by ANI to suspend registration or deregister the organisation.
- Correctly apply the definition of a volunteer, as set out in Regulation 4(d) of the Police Act 1997 (Criminal Records) (Disclosure) Regulations (Northern Ireland 2008), as amended⁷, to each criminal records check

application to ensure that the individual is eligible for an application at no fee

- Where performing an umbrella function on behalf of others, publish all fees, in relevant documentation, associated with the processing and countersigning of criminal records check applications.
- Where performing an umbrella function, notify ANI in writing of these fees or any change to the fees associated with the processing and countersigning of criminal records check applications.

Eligibility

Eligibility for ANI checks is set out in the following legislation:

Standard checks – to be eligible for a standard level ANI certificate, the position must be included in the Rehabilitation of Offenders (Exceptions) (Northern Ireland) Order 1979 (the ROO Exceptions Order).

Enhanced checks – to be eligible for an enhanced level ANI certificate, the position must be included in both the ROO Exceptions Order and Regulation 9 in the Police Act 1997 (Criminal Records) (Disclosure) Regulations (Northern Ireland) 2008, as amended⁸.

⁸ <http://www.legislation.gov.uk/uksi/2009/2495/regulation/2/made> ADD LINK

Enhanced checks with children's and/or adults' barred list check(s) – to be eligible to request a check of the barred lists, the position must be specifically listed in Regulation 9A or 9B of the Police Act 1997 (Criminal Records) (Disclosure) Regulations.

Registered Bodies must:

- Use all reasonable endeavours to ensure that they only submit applications in accordance with the legislative provisions which provide eligibility criteria for relevant positions or employment.
- Ensure that before countersigning an ANI application to be submitted they have assessed the role to be eligible under current legislation, correctly requested the correct level of check, and correctly requested the appropriate barring list information.
- Ensure they are legally entitled to request any ANI certificate applied for.

Compliance Requests

Registered Bodies must co-operate in full and in line with the timescales in current procedures when ANI enquiries are made in relation to:

- Compliance with the obligations under this Code.
- Implementing the suspension or de-registration of a Registered Body where non-compliance is established in line with current procedures.

Data Protection Act 2018

You must have a valid lawful basis in order to process personal data.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

- 1. Most lawful bases require that processing is 'necessary'. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.**
- 2. You must determine your lawful basis before you begin processing, and you should document it. Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason.**
- 3. Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.**
- 4. If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).**
- 5. If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.**
- 6. If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.**