
Vetting & Barring Scheme & Security Screening Policy

1. Introduction

GRAHAM Facilities Management complies fully with the Code of Practice, regarding the correct handling, holding and destroying of Disclosure information, for the purposes of assessing applicants' suitability for employment purposes, voluntary positions, licensing and other relevant purposes. It also complies fully with the Data Protection Act 2018 and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of information and has a written policy on these matters.

We are recognised as a Registered Body, Responsible Body and an Umbrella Body with AccessNI who process criminal record checks on behalf of GRAHAM Facilities Management employees and relevant employees of organisations to whom we sub-contract work.

This policy is available to anyone who wishes to see it on request.

GRAHAM are committed to being an inclusive workplace where all employees, customers and stakeholders can fully participate and contribute. We strive to ensure accessibility across all facets of our operations, including physical spaces, digital platforms, communication channels and services.

Our People policies are regularly audited against rigorous accessibility standards to ensure compliance and to support every employee.

Anyone who requires additional support or has any questions regarding accessibility can contact the HR team at HR-GFM@graham.co.uk

2. Scope

This procedure applies to all employees of the company who will work in positions covered by the:

Northern Ireland

Safeguarding Vulnerable Groups (NI) Order 2007

Protection of Children and Vulnerable Adults (NI) Order 2003 (POCVA)

Rehabilitation of Offenders (Northern Ireland) Order 1978

Scotland

Protection of Vulnerable Groups (Scotland) Act 2007

The Rehabilitation of Offenders Act 1974

England & Wales

Safeguarding Vulnerable Groups Act 2006

UK

Compliance with BS7858 Code of Practice for Security screening of individuals employed in a security environment.

3. Usage

We use disclosure information only for the purpose for which it has been provided. The information provided by an individual for a position within GRAHAM Facilities Management is not used or disclosed in a manner incompatible with the purpose. We process personal data only with the express consent of the individual. We notify the individual of any non-obvious use of the data, including further disclosure to a third party, identifying the Data Controller, the purpose for the processing, and any further relevant information.

4. Handling

GRAHAM Facilities Management recognises that, under section 124 of the Police Act 1997, it is a criminal offence to disclose Disclosure information to any unauthorised person. We, therefore, only pass Disclosure information to those who are authorised to see it in the course of their duties. GRAHAM Facilities Management do not disclose information provided under subsections 112 to 115 of the 1997 Act, namely information which is not included in the Disclosure, to the applicant.

5. Access & Storage

We do not normally retain Disclosure information. If, under certain circumstances as outlined in point 6 below, we do have to retain Disclosure information, it is kept securely in lockable storage units. Access to storage units is strictly controlled to authorized and named individuals who are entitled to see information in the course of their duties.

6. Retention

- AccessNI is an electronic system and paper copies of Disclosure information is provided to the applicant only. GRAHAM Facilities Management can request a copy from the applicant, but this is returned to them following analysis by the HR Department
- If, under certain circumstances, a copy of the disclosure is retained, we do not keep it for any longer than is required after recruitment (or any other relevant) decision has been taken. In general, this is no longer than 6 months. This is to allow for the resolution of any disputes or complaints. Disclosure information will only be retained for a longer than this period in exceptional circumstances which justify retention for a longer period. The same conditions relating to secure storage and access will apply during any such period.

7. Disposal

- Once the retention period has elapsed, we will ensure that Disclosure information is immediately destroyed in a secure manner i.e. by shredding. GRAHAM Facilities Management will ensure that Disclosure information which is awaiting destruction will not be kept accessible to the public or those not authorised to view it e.g. in a waste bin or confidential waste sack.
- We will not retain any image or photocopy, or any other form of the Disclosure information.
- We will, however, keep a record of the date of issue of the Disclosure, the name of the subject, the Disclosure type, the position for which the Disclosure was

requested, the unique reference number of the Disclosure and details of the recruitment decision taken.

8. Disposal

- Applications will be renewed every 3 years where relevant regional legislation requires renewal for Basic, Standard, Enhanced and BS7858 Security Screening.
- It is the employee's responsibility to notify the Human Resources Manager if there are any changes during the interim period e.g. they have been convicted of a criminal offence at any time during the 3-year period. Failure to provide this information may result in disciplinary action.

9. Umbrella Bodies

- Before acting as an Umbrella Body (i.e. a body which countersigns applications for Standard and Enhanced Disclosures on behalf of another organization), GRAHAM Facilities Management will take reasonable steps to ensure that the organisation on whose behalf we are acting will comply with the Code of Practice, and in full accordance with this policy.
- We will also take all reasonable steps to satisfy ourselves that they will handle, use, store, retain and dispose of Disclosure information in full compliance with the Code of Practice, and in full accordance with this policy.
- We will also ensure that anybody or individual at whose request applications for Disclosures are countersigned, has such a written policy and, if necessary, will provide a model policy for that body or individual to use or adapt for this purpose.

10. Employees working in a Security Environment

- Employees working in a Security role will be subject to the SIA Licensing.
- The following list shows the roles that are licensable. If a role you undertake is shown below then you will need a licence if you also undertake a licensable activity. These role definitions are an interpretation for presentational purposes and are produced in good faith. However, the wording in the Private Security Industry Act 2001 always overrides them.

10.1 There are two types of SIA licence:

10.1.1 A front line licence is required if undertaking licensable activity, other than key holding activities (this also covers undertaking non-front line activity). A front line licence is in the form of a credit card sized plastic card that must be work, subject to the licence conditions

10.1.2 A non-front line licence is required for those who manage, supervise and/or employ individuals who engage in licensable activity, as long as front line activity is not carried out – this includes directors* or partners. A non-front line licence is issued in the form of a letter that also covers key holding activities.