An Garda Síochána

Policy Document

Garda National Cyber Crime Bureau

(Including Digital Evidence First Responders)

Effective Date	08/08/2025
Version No.	1.0
Approved by	Garda Executive
Introduced by	HQ Directive 050/2025
Policy Owner	Assistant Commissioner, Organised & Serious Crime

1. Purpose

The Cyber Security role of An Garda Síochána stems from the requirement to safeguard the security of the State under Section 9, of the Policing, Security and Community Safety Act 2024. The purpose of this Policy is to document; the full range of services provided by Garda National Cyber Crime Bureau (GNCCB) and the support provided by Digital Evidence First Responders (DEFRs). The document outlines the process for accessing these services and the criteria GNCCB and DEFR will apply in order to determine the appropriate forensic, investigative or alternate response.

The Garda National Cyber Crime Bureau (GNCCB) through the Cyber Investigations Unit (CIU) is responsible for investigating cybercrimes that contain elements, such as impact, complexity or scale, which would render them unsuitable for investigation by other non-specialist investigation units. The GNCCB define Cyber-dependent crimes as those which can only be committed through use of a computer, computer network or other form of information communications technology. Cyber-enabled crimes are regular crimes that can be committed over or facilitated by a computer network. Where cybercrime offences are investigated by other investigation units; the CIU will provide expert advice and support where necessary.

GNCCB is the principal bureau within An Garda Síochána tasked with conducting forensic examinations of digital media seized or surrendered during the course of criminal or disciplinary investigations. This service is delivered by qualified computer forensic examiners trained in accordance with recognised best practice, supported by processes which ensure the integrity of the examination process from application to completion. The process of forensic examination is supported by locally based resources, the Digital Evidence First Responders (DEFR), who provide an on-the ground service to local investigations and units in the area of computer triage, search and seizure of digital evidence, and cybercrime or cyber forensics awareness.

The GNCCB will compile a regular intelligence programme on cyber matters in cooperation with National and International stakeholders, including academia, industry and law enforcement partners. This will ensure that regular intelligence updates are available for review and distribution on cyber trends and offending, to inform and assist GNCCB operations. This intelligence gathering will include all available sources, including open source intelligence and partner communications.

The provision of Cyber Safety advice to the public and external stakeholders is a central activity of the bureau. The proliferation and continuing development in the areas of cybercrime and evolution of cyber security threats requires the GNCCB to engage with its stakeholders, advising of the latest identified cyber trends and threats.

GNCCB acts as the primary reference point in respect of cyber-related matters. The bureau engages with other designated national central reference points, and with Europol and INTERPOL. In this capacity, GNCCB adopts an active role in engagement with external stakeholders on this topic, particularly those that have an active interest or role in this specialist environment. GNCCB also provides training and advice, internally within An Garda Síochána, to assist Garda personnel in providing an appropriate investigative response in respect of cybercrime incidents.

2. Scope

This Policy and all associated documentation apply to all Garda members and Garda Staff. It also applies to Police Officers from the Police Service of Northern Ireland (PSNI) seconded to An Garda Síochána in accordance with Section 94, of the Policing, Security and Community Safety Act 2024.

3. Policy Statement

An Garda Síochána has an obligation to conduct cybercrime investigations and the forensic examination of all digital media seized during criminal investigations in an independent and impartial manner where integrity, transparency and accountability are evident within every aspect of the processes deployed. GNCCB have been delegated with responsibility for this task on behalf of An Garda Síochána. The procedures adopted by GNCCB (including DEFRs) in fulfilling this role ensures that all investigations they conduct are carried out in accordance with recognised and approved investigative best practice. They also ensure that all digital media exhibits received within the bureau are subject to a rigorous examination process, whilst ensuring that each of the above purposes are consistently maintained.

GNCCB will ensure that all applications for assistance are considered in a fair and equitable manner. All applications for assistance must be made in the designated manner, which is then subject to assessment. The response provided, across all of the bureau's designated service areas, is based on the level of perceived risk that is evident within each individual application. This assessment process ensures fairness and equitability; whilst maximising the operational functionality of the GNCCB. This service is supported by Divisional based DEFR's who are trained in computer triage processes, digital evidence search, preservation and seizure procedures, and computer technology. The DEFR members act as an initial first point of service to local units and investigations on all aspects of computer based or related investigations.

4. Compliance

Compliance with this Policy and accompanying Procedures is mandatory for all members of An Garda Síochána, Garda Staff and Police Officers from the Police Service of Northern Ireland (PSNI) seconded to An Garda Síochána in accordance with Section 94, of the Policing, Security and Community Safety Act 2024.

5. Related Documents

- GNCCB Procedure Document
- Garda National Cyber Crime Bureau: Forensic Examination Application Form
- Garda National Cyber Crime Bureau: Cybercrime Incident Investigation Matrix
- Data Protection Act 1988
- Data Protection Act 2003
- Data Protection Act 2018
- Data Protection Code of Practice for the Garda Síochána
- Freedom of Information Code of Practice
- An Garda Síochána Code
- Code of Ethics for the Garda Síochána
- Garda Decision Making Model
- HQ Directive 47/95 - National Archiving Act 1986
- HQ Directive 95/2012 - Data Protection in An Garda Síochána

- HQ Directive 40/2014 - Data Protection in An Garda Síochána – Confidential Reporting and Data Protection legislation
- HQ Directive 87/2015 - Freedom of Information Act 2014 (Implementation in An Garda Síochána)
- HQ Directive 19/19 - Human Rights Framework - Human Rights Screening Tool; '*A Human Rights Based Approach to Policing'* – Operational Guidance Document
- The European Court of Human Rights

6. Cancelled Documents

- HQ Directive 01/2004 - Applications to Garda Bureau of Fraud Investigation requesting the assistance of the Computer Crime Investigation Unit (C.C.I.U.)

7. Legal & Human Rights Screened

This Policy and the associated procedures document, have been screened in terms of the respective obligations placed on An Garda Síochána, for the subject area concerned.

8. Ethical Standards and Commitments

Every person working in An Garda Síochána must observe and adhere to the standards and commitments set out in the Code of Ethics for An Garda Síochána and uphold and promote this code throughout the organisation.

9. Policy & Procedure Review

This Policy and associated document(s) will be reviewed 12 months from its date of effect and every three years thereafter, or as appropriate.

10. Disclaimer

This document is not intended to, nor does it represent legal advice to the relied upon in respect of the subject matter contained herein. This document should not be used as a substitute for professional legal advice.

11. General Data Protection Regulation & Data Protection Acts 1988-2018

All Garda personnel will process personal data for specified purposes only and within a clearly defined lawful basis under the General Data Protection Regulation ((EU) 2016/679) and Data Protection Acts 1988/2018. All necessary measures will be put in place to ensure the personal data is kept safe and secure and only authorised personnel shall have access to personal data. Only relevant personal data will be processed, and will not be retained for longer than is necessary. All personnel are required to ensure that individual's data protection rights are adhered to and to identify and mitigate against any suspected data breaches.