Nottinghamshire County Council

Information Security Policy

Context

1. Information is a critical asset for Nottinghamshire County Council (NCC). The security of information assets, as well as the supporting processes, systems and networks, is essential to maintaining operational effectiveness, reputation, financial accuracy and legal compliance.

2. NCC are subjected to a wide variety of sophisticated security threats, including malware, hackers and computer-assisted fraud. The dependence on data, information systems and services means that NCC are ever more vulnerable to these threats.

3. The requirement to interconnect the NCC network with suppliers and partners, alongside the growing use of Cloud services, makes security increasingly complex.

4. The objective of information security is therefore to achieve and maintain a condition where all information is available at all times to all those who need it, cannot be corrupted or disclosed to unauthorised persons and its origin is authenticated. This involves the preservation of:

    - **Confidentiality** - ensuring that information is only accessible to authorised persons;
    - **Integrity** - safeguarding the accuracy and completeness of information and processing methods;
    - **Availability** - ensuring that authorised users have access to information and associated assets when required;
    - **Non-repudiation** – the reasonable assurance that, where appropriate, a user cannot deny being the originator of a message after sending it.

5. It is important that information security is appropriate, proportionate, integrated and coordinated. It should enhance business processes, rather than impede them.

Scope of this policy

6. The policy applies to all NCC data and systems, and to all NCC personnel with access to NCC data or systems, irrespective of status, including temporary staff, contractors, consultants, and third parties.

Principles and Commitments

7. The Information Security Policy is Mandatory. It must be read and understood by all NCC employees who use, or may need to use, IT systems, information and services at NCC. Wilful or negligent disregard for information governance policies and procedures by employees will be investigated and may be treated as a disciplinary matter which could lead to dismissal.

8. All regulatory and legislative requirements must be met.

9. All users of IT systems are accountable for their actions.

10. All users of IT systems should receive appropriate training and regular updates in organisational IT security policy, standards and procedures.

11. All information must be handled in a way appropriate to its sensitivity, in accordance with the Information Classification and Handling Standard.

12. All hardware and software must be kept up to date to minimise the likelihood of security vulnerabilities being exploited, in accordance with the Patching Standard.

13. IT equipment must be properly configured and managed to reduce the risk of malware and other security threats, in accordance with the Network Security Standard.

14. Users must only be granted access to the IT systems and data necessary to fulfil their role, in accordance with the Access Control Standard.

15. Remote access services must be configured to minimise opportunities for unauthorised access or denial of service, in accordance with the Remote Access Standard.

16. Resources which are hosted in Cloud Computing environments must be maintained to an acceptable level of security, in accordance with the Cloud Security Standard.

17. All IT equipment must be adequately secured to prevent theft, and critical IT infrastructure must be physically secured to prevent unauthorised access, in accordance with the Physical Security Standard.

18. Controls must be implemented to reduce the risk to the confidentiality, integrity and availability of IT systems and data caused by malicious software (malware), in accordance with the Anti-Malware Standard.

19. All IT systems must be designed, configured and managed to minimise opportunities for unauthorised access or denial of service, in accordance with the System Configuration and Management Standard.

20. The use of passwords must be managed to minimise the risk of unauthorised access to IT systems or data, in accordance with the Password Standard.

21. Encryption techniques must be used to protect sensitive information, in accordance with the Encryption Standard.

22. Systems must be monitored to ensure malicious activity is detected, in accordance with the Protective Monitoring Standard.

23. Users of IT systems, including e-mail and the Internet, must use these systems in a way that minimises the risk to the confidentiality, integrity and availability of IT systems and information, in accordance with the Acceptable Use Standard.

24. Controls must be applied to prevent unauthorised access to information stored on removeable media, and to reduce the risk to NCC systems from data originating from removeable media, in accordance with the Removable Media Standard.

25. Third party access to NCC systems must be authorised and controlled, and third parties with such access must adhere to all other NCC policies, in accordance with the Third Party Access Standard.

26. Information must be kept for a period of time described by the Information Retention Standard. Information, systems and hardware that is no longer required must be securely destroyed in accordance with the Data Destruction Standard.

27. All security incidents must be handled in accordance with the Incident Response Standard.

28. Controls must be implemented to minimise the impact of any system unavailability, in accordance with the ICT Business Continuity Standard.

29. Personally Owned Devices are only permitted to access the NCC network, and NCC applications, either located on the NCC network or in the Cloud as part of the NCC approved Bring Your Own Device (BYOD) service, in accordance with the BYOD Standard.

Owner	Data Protection Officer
Author	Chris Towner, Information Security Architect
Last Reviewer	Chris Towner, Information Security Architect
Approver	Senior Information Risk Owner (SIRO) under delegation from Policy Committee
Date of Approval	24/10/2022
Date of next review	24/10/2023
Version	1.2
Classification	Public

Version	**Date**	**Changes**

1.0	28/03/18	Original document approved by Policy Committee
1.1	30/1019	Minor format changes and document control table added at end.
1.2	8/9/2022	Clause 29 added to refer to the new BYOD Standard.