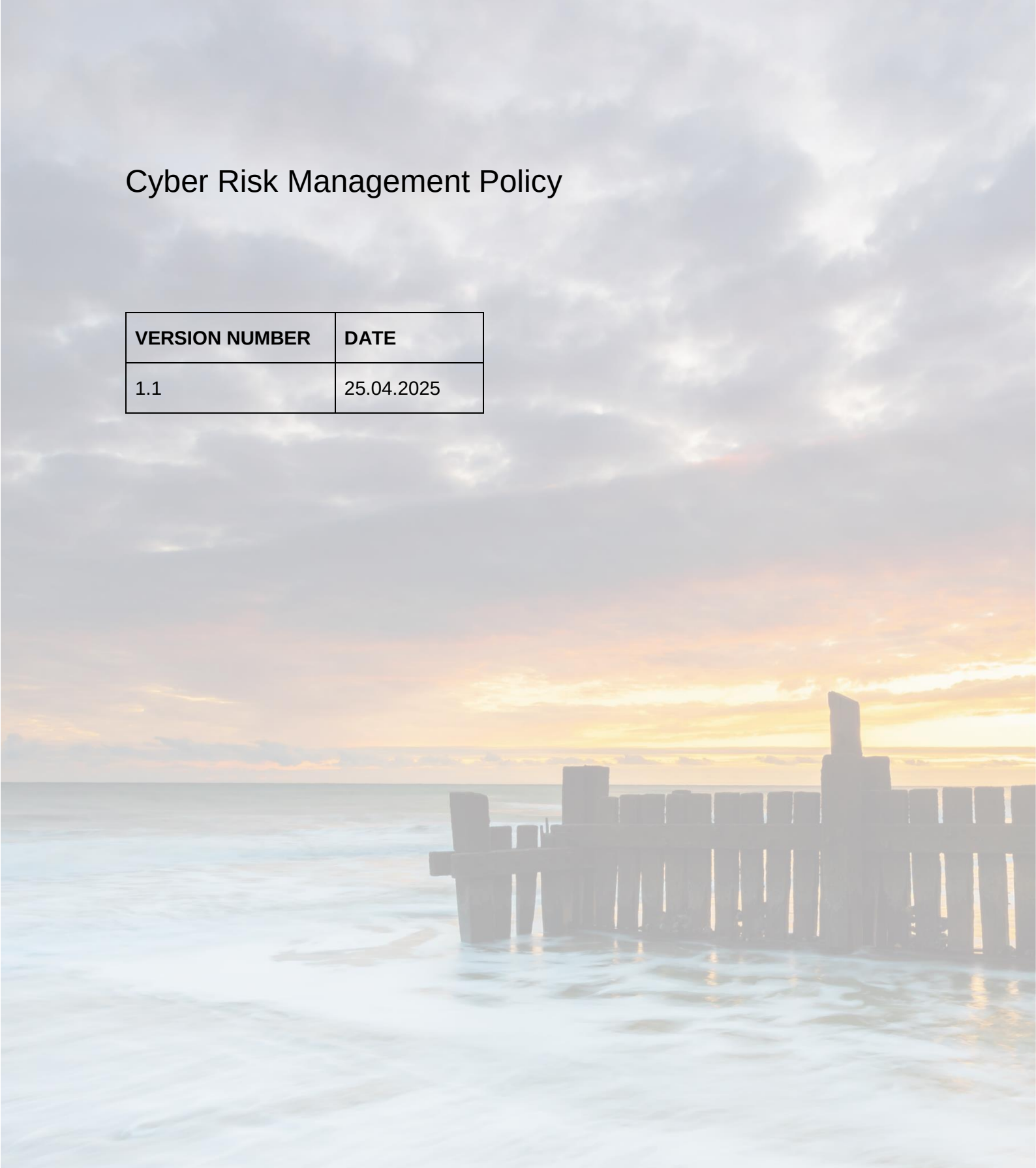
Cyber Risk Management Policy

VERSION NUMBER	DATE
1.1	25.04.2025



NORTH NORFOLK DISTRICT COUNCIL

Cyber Risk Management Policy

PUBLICATION DATE

VERSION NUMBER	DATE
1.1	25.04.2025

Foreword

Digital services are integral to delivering modern, effective public services. With increasing cyber threats, it is essential that North Norfolk District Council takes a proactive and structured approach to managing cyber risks. This policy sets out our commitment to safeguarding the authority's digital infrastructure, data and service continuity.

Contents

Executive Summary

This policy outlines the framework for identifying, assessing, and mitigating cyber risks to ensure the security and resilience of North Norfolk District Council against evolving cyber threats. It defines responsibilities for cyber risk management, ensures compliance with legal and regulatory requirements and supports our goal of maintaining public trust and operational resilience.

The Council recognises that regular cyber risk assessments are essential for establishing a risk baseline, maintaining compliance, and safeguarding critical data and infrastructure.

Scope

This policy applies to all employees, elected members, contractors, and third-party vendors who access IT infrastructure, data, or digital assets owned or managed by North Norfolk District Council. It encompasses all forms of cyber risk, including but not limited to ransomware, phishing, denial-of-service attacks, insider threats, and data breaches.

Policy Statement

North Norfolk District Council is committed to proactive and robust cyber risk management. This includes:

- Protecting information, systems, and services from evolving cyber threats.
- Integrating cyber risk management into the Council's broader corporate risk governance and service delivery.
- Complying with relevant UK legislation and standards, including the Data Protection Act 2018, UK GDPR, and PSN compliance.
- Promoting a culture of cyber awareness and resilience across all services.

Cyber Risk Management Framework

Cyber risks will be managed through a structured process involving:

1. Risk Identification

- Continuous monitoring of ICT infrastructure using internal and external tools.
- Proactive use of system alerts directed to a monitored security mailbox (7 days/week, 8am–5pm).
- Maximising in-built security features (e.g. Microsoft Enterprise E5).
- Regular vulnerability scanning and threat intelligence updates.
- Routine patching and adherence to the Patching Policy.

2. Risk Assessment

- Risks are assessed based on impact and likelihood using established methodologies.
- Strategic risks are recorded on the Corporate Risk Register, while operational and ICT-specific risks are tracked on the Departmental Risk Register and a dedicated Cyber Security Risk Register, reviewed quarterly by the ICT service.
- The Council prioritises risks that could affect service delivery, data integrity, or public trust.

3. Risk Mitigation

- Access Control & Authentication: Enforce strong password policies, multi-factor authentication (MFA), and role-based access controls.
- Data Protection: Encryption of sensitive data in transit, at rest, and on mobile devices; alignment with the Backup Policy and Business Continuity Plan.
- Network Security: Network traffic monitoring and protection against unauthorised access (as detailed in the Logging and Protective Monitoring Policy).
- Incident Recovery: Proven backup regimes and tested recovery procedures ensure rapid restoration following a cyber event.

Roles & Responsibilities

Cyber risk management is a shared responsibility across the whole authority:

Chief Executive

- Provides strategic oversight and ensures cyber resilience is prioritised across the Council.

Senior information Risk Owner (SIRO)

- Leads cyber governance and integrates cyber risk into the wider risk management framework.

Corporate Leadership Team

- Allocates resources and supports effective cyber risk management across departments.

Strategic ICT Manager

- Oversees technical controls, incident response planning, and delivery of risk assessments.

ICT Team

- Implements updates and upgrades to mitigate risks.
- Manages cyber risks from external suppliers, including during procurement.
- Oversees system patching, monitoring, and threat intelligence.
- Maintains the Cyber Threat Register.
- Represents the Council at the Norfolk Cyber Delivery Group and Cybershare East, ensuring awareness of emerging threats.
- Maintain awareness of Norfolk Resilience Forum (NRF) Cyber Resilience Plan and take part in any exercises organised.

Service Managers

- Identify service-specific cyber risks and ensure appropriate local controls are applied.

All staff and councillors

- Comply with all security policies, including IT Security and Information Incident Management procedures.
- Complete mandatory cyber awareness training within required timeframes.
- Respond appropriately to simulations that have been designed to educate users of phishing risks.
- Report suspicious activity promptly.

Equality Impact Analysis

This policy aims to achieve effective management of Cyber Risk while ensuring that it does not create any unnecessary barriers for individuals with protected characteristics. No adverse impacts on protected groups have been identified. Reasonable adjustments will made as required to ensure digital and training accessibility for all service users. The policy will be subject to ongoing monitoring and evaluation, with any findings used to inform future policy development and implementation.

Review Process

This policy will be reviewed annually, or sooner if triggered by:

- Significant changes to the threat landscape.
- Legislative or regulatory developments.
- Major changes in Council infrastructure or services.
- Findings from internal or external audits.

Ongoing monitoring is embedded in ICT operations. All high-priority alerts will be directed to a designated mailbox monitored during working hours and weekends.

Distribution & Amendment

This policy will be made available through:

- The Council's intranet.
- Induction and training materials.
- Email communication to managers and stakeholders.

All changes will be documented in the Version Control section and communicated following approval by the appropriate governance group.

Document Information & Version Control

Document Name	Cyber Risk Management Policy
Document Description	Cyber Risk Management Policy
Document Status	Current
Lead Officer	Kate Wilson
Sponsor	Dan King
Produced by (service name)	IT
Relevant to the services listed or all NNDC	All NNDC
Approved by	CLT
Approval date	
Type of document	Policy
Equality Impact Assessment Details	Current
Review Interval	2 years
Next Review Date	01/04/2027

Version	Originator	Description including reason for changes	Date
1.0	KW/HC	Draft policy submitted	25/04/2025
1.1	KW	Changes to reflect change of AD & TS leaving	09/06/25