Gateshead Council

REPORT TO CABINET
19 March 2024

TITLE OF REPORT: Information Security Framework and Policy

REPORT OF: Darren Collins, Strategic Director, Resources and Digital

---

Purpose of the report

1. To recommend to Cabinet and Council a new Information Security Framework and Associated IT Security Policies and the approach to implementing the new framework and associated policies.

Background

2. It is important that the Council has an IT Security Policy which identifies the requirements for all individuals accessing and using the Council's IT assets and resources (IT users) in order to preserve the confidentiality, integrity, and availability of systems and information used by the Council.

3. The IT Security Policy demonstrates the commitment of the highest level of leadership within the organisation to the ideals of the policy, therefore providing direction for the rest of the employees, suppliers, and other stakeholders

4. The landscape of IT technologies and services is forever changing and at a rapid pace and, whilst the old policy has served its purpose, it has become outdated and does not cover some of the technologies we've come to heavily rely on, such as cloud services.

5. The Council's Cyber Security Group have been working on creating the new IT Security Policy and associated policies for the past 18 months.

Proposal

6. It is proposed that the council implement a new IT Security Framework for all IT Users consisting of a main IT Security Policy and eight sub policies relating to specific activities or functions within the council. The sub policies are as follows

   - Acceptable Use Policy
   - Personnel Security Policy
   - Remote working Security Policy
   - Email Policy
   - SMS Policy
   - Social Media Policy
   - IT Asset Management Policy
   - Information Classification Policy

7. The new policies can be found in appendix 2.

8. Additional policies will be added to the framework when technologies change. Other new or updated policies also exist but they do not apply to all IT users.

9. Roles and responsibilities are clearly identified in the new IT Security Policy, with Information Asset Owners (Service Directors) having specific responsibilities. A dedicated learning package will be available to Service Directors to ensure they understand their responsibilities.

10. An awareness programme will take place using the Intranet, Council Info and employee forums and focus groups to communicate the changes to all stakeholders.

11. All policies will be reviewed on an annual basis (or earlier should changes to technology or legislation necessitate this) by the Councils Cyber Security Group.

12. IT users will be asked to accept the policies on an annual basis using a policy acceptance application.

Recommendations

13. That Cabinet recommends Council to approve the new IT Security Framework and Policy as set out in appendix 2 and the approach to implementing the new framework and associated policies to safeguard the Councils Information Assets and Technologies.

    For the following reasons

    To preserve the confidentiality, integrity and availability of the councils information assets enabling services to deliver the Thrive Agenda and the Council Plan, and protecting those whose information we hold.

CONTACT: Joanne Morgan Extension 3716

APPENDIX 1

Policy Context

1. Confidentiality, integrity and availability of the council's information systems and assets is crucial in enabling services to support the delivery of the Council's Thrive agenda and the Corporate Plan 2023 – 2028.

Background

2. An IT Security Policy identifies the requirements for all individuals accessing and using an organisation's IT assets and resources and is a model of the organisation's culture, in which rules and procedures are driven from its employees' approach to their information and work.

3. An organisations IT Security Policy demonstrates the commitment by the highest level of leadership within the organisation to the ideals of the policy, therefore providing direction for the rest of the employees, suppliers, and other stakeholders

4. The objective of an IT Security Policy is the preservation of confidentiality, integrity, and availability (CIA) of systems and information used by an organisation's members.

    - Confidentiality - involves the protection of assets from unauthorised entities.
    - Integrity - ensures the modification of assets is handled in a specified and authorised manner.
    - Availability - is a state of the system in which authorised users have continuous access to said assets.

5. The IT Security Policy must be a living document that is continually updated to adapt with evolving business and IT requirements and in line with defence from evolving cyber security threats and risks.

6. An organisation's IT Security Policy will play a large role in its decisions and direction, but it should not alter its strategy or mission. Therefore, it is important that any policy is drawn from the organisation's existing cultural and structural framework to support the continuity of good productivity and innovation, and not as a generic policy that impedes the organisation and its people from meeting its mission and goals.

Planned Changes

7. The landscape of IT technologies and services is forever changing and at a rapid pace and, whilst the old policy has served its purpose, it has become outdated and does not cover some of the technologies we've come to heavily rely on, such as cloud services.

8. The Council's Cyber Security Group have been working on updating the old IT Security Policy for the past 18 months.

9. The group consists of officers from IT Services, Legal and Demographic Services, Human Resources and Workforce Development, Internal Audit and Risk, Insurance and Communications.

10. From a very early stage, it was decided that we needed to break down the old Policy into a framework with a number of dedicated, bite-sized and easier to understand policies. This change to a framework subsequently also became an audit requirement.

Policy Structure

11. The Council's new Information Governance Framework sits above the Data Protection policy and this new IT Security Policy Framework.

12. The new IT Security Policy framework consists of the main IT Security Policy and currently eight sub policies, all relating to specific activities or functions within the Council.

Information Governance Framework	
Data Protection Policy	IT Security Policy
	• Acceptable Use Policy • Personnel Security Policy • Remote working Security Policy • Email Policy • SMS Policy • Social Media Policy • IT Asset Management Policy • Information Classification Policy

13. An additional Artificial Intelligence (AI) policy is also in draft and will be added to this Framework once complete.

14. At a minimum, each policy consists of the following sections:

- **Purpose** – Why the policy exists and what it aims to achieve.
- **Scope** – Who and what the policy applies to.
- **Policy Statements** – the actual declaration of intent of the Council
- **Responsibilities** – A list of responsibilities
- **Compliance** – confirmation that all employees are responsible for compliance with each policy
- **Non-Compliance** – confirmation that non-compliance will be deemed an intrusion attempt or a breach of security
- **Policy Acceptance** – All users are required to confirm that they have read and understood each policy

15. Other new or updated policies also exist but they do not apply to all users. For example, privileged user security policy, system owners policy, technical vulnerability management policy and more.

IT Security policy

16. **Purpose** - The purpose of this policy is to define the overarching cyber security requirements necessary to safeguard all council IT resources.

17. **Scope** - It covers all users who have been granted access to any council IT resource.

18. It does not replace any of the Council's legal or regulatory requirements

19. **Policy Statements** - The policy statements are the Council's high level declaration, written to cover all areas of IT security.

20. **Roles and Responsibilities** - Roles are required within the Council to provide clearly defined responsibilities and an understanding of how the protection of information is to be accomplished

21. We all have some IT Security responsibilities, either based on the service we work in, the working groups we're a member of, the sensitive information we have access to or simply because we have access to any Council digital resource. It is essential that these responsibilities are clearly defined and communicated throughout the business on a recurring basis.

22. The newly documented roles and responsibilities are perhaps the most important aspect of the new top-level IT Security Policy.

23. There are some very important roles and groups mentioned such as the Chief Executive, the Senior Information Risk Officer (SIRO), Corporate Risk and Resilience Management Group, the Cyber Security Group, the Corporate Data Protection Group and more.

24. However, those who can have the biggest impact on the Council's entire Cyber Security posture at this moment in time are the Information Asset Owners - our service directors who are responsible for the Council's digital assets, both cloud-hosted and on-premise.

25. Some of these key areas of responsibility include:
    - Leading and fostering a culture that promotes good cyber security practices across their service.
    - Ensuring appropriate identity and access controls are implemented for their assets.
    - Understanding and addressing cyber risks to the asset, including vulnerability management, and providing assurance to the SIRO.
    - Ensuring that all applications, systems and services used to process data are appropriately maintained and supported at all times.
    - Understanding how and where data flows between their assets.
    - Ensuring that information governance policies and procedures are implemented across all digital assets including, classification and retention.
    - Appointing an appropriately knowledgeable System Owner for all applications and systems owned by the service.
    - Ensuring that an appropriate and tested business continuity framework (both strategic and operational) exists for all critical systems owned by the service
    - Ensuring that all third parties involved the processing of service data are aware of their roles and responsibilities.

26. The Council's Cyber Security Group and IT Services are in the process of creating a dedicated learning package on the Council's Learning Hub, which aims to help Service Directors understand their responsibilities within these areas.

27. **Breaches of Security** – This section explains the reporting procedures as well as the action that might be taken in the event of a breach of policy. For consistency, all other sub-policies refer to these actions within their non-compliance sections.

Implementation

28. It is proposed that these changes are introduced on 1st April 2024

Consultation

29. The Leader of the Council, Deputy Leader of the Council, Corporate Management TeamTrade Unions and the Cyber Security Group have been consulted on the Framework and associated policies.

30. We will inform employees of the new policies via Council Info, Intranet and Learning Packages on the Learning Hub if the approach is endorsed.

Alternative Options

31. One alternative option could be to retain the current IT Security Policy, however this is not recommended as it would pose a significant risk to the Council in relation to an increased likelihood of a successful Cyber Attack or Data Loss/Breach.

Implications of Recommended Option

32. **Resources**
a) Financial Implications - The Strategic Director, Resources & Digital confirms that there are no financial implications arising from this report.

b) Human Resources Implications – There could be human resources implications arising from this report. Should an employee fail to adhere to the policies, disciplinary action could result, following a formal investigation.

c) Property Implications – There are no property implications arising from this report.

33. **Risk Management Implication** – Introduction of the new IT Security Framework will reduce the risk of a successful cyber-attack or significant data breach/loss.

34. **Equality and Diversity Implications** - There are no equality and diversity implications arising from this report.

35. **Crime and Disorder Implications** - There are no crime and disorder implications arising from this report.

36. **Health Implications** – There are no health implications arising from this report.

37. **Climate Emergency & Sustainability Implications** – There are no climate change implications arising directly from this report.

38. **Human Rights Implications** - Human rights implications could arise from this report. Should an investigation be required into an individuals alleged misuse of Council IT resources investigators could be subjected to personal information. This is clearly documented in the IT Security Policy and strict processes exist to ensure investigations take place in line with Council policy.

39. **Ward Implications** - There are no ward implications arising from this report.

Appendix 2

Gateshead Council

Information Technology (IT) Security Policy

Introduction by the Leader of the Council and the Chief Executive

The Council recognises the growing demand for digital services and technologies which prompts important opportunities for the Council. Information held within IT systems and cloud services is a key resource and we must make sure that it is used appropriately and securely, and that the Council is protected against potential security threats.

This revised IT Security Policy along with its related sub polices sets out the Council's approach to cyber security and aims to support the Council's wider commitment to managing threats and opportunities as set out in its Corporate Risk Management Policy. It is intended that this policy will help councillors and employees to understand the risks and implications of using IT resources and their responsibilities in relation to its use.

It is important that we all take our responsibilities seriously, as we want everyone to be able to work with the many types of technology available to the Council in a safe and secure environment. All employees are responsible for making sure that the policies are put into practice.

Please read this policy and all supporting sub policies to help ensure that the Council's data is securely protected in accordance with legislation such as the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

Additional guidance relating to Information and Cyber Security can be found on the Intranet. If there is anything you don't understand, please talk to your line manager. We are sure that with the co-operation of everyone, this policy will improve cyber security throughout the Council.

Councillor Martin Gannon
Leader of the Council

Sheena Ramsey
Chief Executive

Purpose

The growing demand for digital services and technologies prompts important opportunities for the Council, but also leads to a greater “attack surface” that requires enhanced cyber security measures to minimise risks. Inconsistent management of IT resources has the potential to increase the risk of a cyber-attack or lead to the compromise of Council data.

The purpose of this IT Security Policy along with its supporting standards and guidelines, is to define the overarching cyber security requirement necessary to safeguard ALL IT resources and to ensure the confidentiality, integrity and availability of the information held therein.

In this policy the expressions “Council” or “Gateshead Council” includes any agents, third-party organisation or company that utilises Gateshead Council’s IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Scope

This policy sits below the Council’s overarching Information Governance Framework and applies to all IT resource that stores or processes Council data.

For the purposes of this policy, IT resources can include but is not limited to user accounts, end-user devices, systems, applications, networks, cloud resources, printers, telephones and customer facing web services.

This policy is mandatory for all persons who have been granted access to any Council IT resources.

Legislation

Gateshead Council has an obligation to abide by all relevant legislation, all members of staff must abide by UK legislation relevant to information security including:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Computer Misuse Act 1990
- Electronic Communications Act 2000
- Copyright, Designs and Patents Act 1988
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Civil Contingencies Act 2004
- Freedom of Information Act 2000

All Service areas must also comply with any specific information protection standards relevant to Council business.

Definitions

A list of terms used throughout this policy are defined in within **Appendix A**.

Policy Statements

It is the policy of Gateshead Council to: -

- Develop and maintain appropriate policies, standards, procedures and guidelines to affect a high standard of cyber security, reflecting industry best practice.
- Implement human, organisational, physical and technological security controls to preserve the confidentiality, integrity and availability of its IT resources and the information held therein.
- Maintain a thorough understanding of the IT resources we manage, and what business need they support.
- Maintain a strong and thorough vulnerability management programme covering all IT resources.
- Utilise appropriate identity and access mechanisms for all IT resources.
- Maintain an Information and Cyber Security awareness programme across all users with access to IT resources.
- Monitor, record and log activity on the Council's network and use of its IT resources.
- Rapidly detect and determine the cause of any breach of security and aim to minimize damage to IT resources should any such incident occur.
- Only use supported IT resources to store or process Council information.
- Work closely with the suppliers of our products, systems and services to help improve security across our supply chain.
- Comprehensively assess and manage cyber risks to safeguard IT resources and the information held therein. This includes the continuous review and improvement of Cyber security controls.
- Comply with all relevant laws and regulations.

Roles & Responsibilities

CEO
The Chief Executive has overall accountability for information governance.

SIRO
The SIRO is a Senior Leadership Team member responsible for managing information risk at the highest level. Key responsibilities are to:

- Oversee the development of information governance policies and information risk management strategy
- Ensure that the Council's approach to information risk is effective, in terms of resource, commitment and delivery
- Ensure that all staff are aware of the necessity for information governance and the risks affecting the Council's information.
- Provide a focal point for managing information risks and learning from incidents
- Prepare an annual information risk assessment for the Chief Executive to be included in the Annual Governance Statement

Information Governance Board
The Information Governance Board provides overall direction and leadership for information governance arrangements. The Board is chaired by the SIRO, who is supported by professional and business leads. Key responsibilities are to:

- Lead and influence the direction of information governance
- Provide overall strategic direction and alignment of information governance with other organisational change work

- Work collaboratively to ensure successful information governance delivery
- Ensure that information governance is appropriately resourced
- Own the resolution of information governance issues, risks and decisions.

Audit and Standards Committee (Risk Management Assurance)

The Audit and Standards Committee is the principal interface with Councillors for the purposes of supporting and monitoring the Council's risk management arrangements. The Committee receives quarterly reports on the Council's performance in relation to risk management and this provides an opportunity for challenge and discussion.

Cyber Security Group

The Cyber Security Group is responsible for agreeing the most appropriate technical controls to implement across Council managed systems and devices:

- To meet legal compliance requirements
- For compliance with external standards
- In line with internal information management policies
- Following an incident review
- In line with Cyber Security best practice

The Group will also assist services throughout the Council with their own Cyber Security responsibilities for non-Council managed systems and devices. This may include assistance with:

- Cyber risk management requirements
- Incident management
- Appraisal of corporate systems
- Penetration testing and mitigation requirements of corporate systems

Corporate Risk and Resilience Management Group

The Corporate Risk and Resilience Management Group is an officer group consisting of the central risk management function, all Risk and Resilience Co-ordinators and representatives from the Council's Corporate Resilience Planning Team and IT Services. As part of its role and remit the group will assist with the comprehensive assessment and management of cyber risks to safeguard IT resources and the information held therein.

Corporate Data Protection Group

The purpose of the Corporate Data Protection Group (CDPG) is to ensure cross-council compliance with data protection obligations. The CDPG is to demonstrate accountability for the data protection principles which the Council must follow when processing personal data. As data protection is the responsibility of every employee of the Council, the CDPG will ensure that the key data protection principles are applied across the organisation. The role of the Corporate Data Protection Group is to:

- ensure that the Council's information governance framework is complied with
- ensure that the Council's approach to handling personal data is reflective of national standards and is communicated to all staff and made available to the public
- ensure the recommendations of the Information Governance / Data Protection internal audit are fulfilled
- offer support, advice and guidance concerning Data Protection, Freedom of Information and Subject Access issues within the Council
- monitor the Council's information handling activities to ensure compliance with law
- monitor reviews/audits relating to information governance and adherence/development to relevant standards

- review and discuss lessons learnt from data breach incidents to ensure the risk of future incidents is mitigated.

Information Asset Owners

Information Asset Owners are Service Directors responsible for ALL information assets including digital assets (cloud hosted and on-premise) and assessing, controlling and mitigating cyber risks in their service areas. Key responsibilities include:

- Leading and fostering a culture that promotes good cyber security practices across their service.
- Maintaining a thorough understanding of the IT resources used within their service and what business need they support.
- Ensuring appropriate identity and access controls are implemented for their assets.
- Understanding and addressing cyber risks to the asset, including vulnerability management, and providing assurance to the SIRO.
- Ensuring that all applications, systems and services used to process data are appropriately maintained and supported at all times.
- Understanding how and where data flows between their assets.
- Ensuring that information governance policies and procedures are implemented across all digital assets including classification and retention.
- Appointing an appropriately knowledgeable System Owner for all applications and systems owned by the service.
- Ensuring that there are handover processes in place should key parties leave.
- Ensuring that an appropriate and tested business continuity framework (both strategic and operational) exists for all critical systems owned by the service.
- Ensuring that all third parties involved the processing of service data, wherever located, are aware of their roles and responsibilities.

Information Asset Assistants

Information Asset Assistants are operational members of staff nominated by Information Asset Owners. Key responsibilities include:

- Acting as a local contact for Cyber Security in their service area.
- Supporting the IAO in identifying and addressing cyber risks.

Internal Audit and Risk Management

Internal Audit and Risk provide assurance that information technology controls and procedures are operated in accordance with the policies, regulations and best practice.

Internal Audit is statutory service in the context of the Accounts and Audit Regulations (England) 2015. And the Public Sector Internal Audit Standards defines the role as: “Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation’s operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes”
Risk management is one of the key systems within the Council and the risk management responsibilities are set out in the Council’s Financial Regulations.
Legal and Democratic Services

Legal and Democratic Services provide training and advice on data protection matters and Freedom of Information Act requests; they liaise with and advise senior management, individual users and line managers on relevant laws and regulations; assist in the development of data related policies and procedures, and advise on appropriate actions to take in the event of an actual or suspected breach data security.

The Council Data Protection Officer sits within Legal and Democratic Service.

Human Resources

Human Resources provides a range of services, relating to improving the employee experience for our people across the Council.

They work collaboratively and in partnership with every Service Director, their leadership teams, managers, our people and our recognised trade unions to improve every aspect of the employee life cycle taking both a tactical and strategic approach to transforming and continuously improving the people experience.

They ensure that cyber security is covered throughout the staff lifecycle with appropriate guidelines, policy and support for the workforce. This includes:

- Ensuring the Council has a policy and procedure in place in relation to recruitment including all relevant pre-employment checks
- Ensuring that staff are encouraged to speak up, to raise problems and voice new ideas.
- Encouraging staff at all levels to complete relevant training issued via Learning Hub.
- Ensuring that the Council has an appropriate Disciplinary Policy and Procedure which is made available to managers and staff.
- Overall ensuring in conjunction with HR Support and Payroll that there are procedures in place in relation to management of joiners, transfers and leavers.

IT Services

IT Services provide strategic planning, development, implementation and support of information and communication technology solutions for the council, schools and other key customers.

The Cyber Security team within IT Services implement the technical solutions required to assist with identifying vulnerabilities and securing the Councils on premise IT solutions, and work with services to ensure that the appropriate technical controls exist and are implemented for the cloud hosted solutions they may use to process and store their data.

IT Services also ensure that physical environmental controls protect our datacentres to protect against tampering, fire, flood and theft.

Corporate Communications

The Corporate Communications team plays a key role in managing and overseeing the council's reputation - both on a local, regional, and national scale.

The team provides a professional communications service to all council service areas and partner agencies to ensure that Gateshead residents, businesses, colleagues, and the media are provided with accurate and up-to-date information about council services, facilities, and policies.

The Corporate Communications team is responsible for:

- handling media enquiries from local, regional, and national newspapers, television, and radio stations
- providing advice on media issues
- issuing press releases
- providing professional help and advice to officers and councillors
- conducting daily media monitoring, including social media
- creating and managing a wide range of marketing campaigns
- graphic design
- internal communication to colleagues through a range of internal channels
- producing the Council's main print and digital publications, including Council News and Gateshead Now

System owners

System owners are responsible for ensuring that the controls identified in this policy and the IT System Owner Policy are implemented at a level appropriate for the risks to the system and the information it processes.

Line managers

Line Managers are responsible for:

- The implementation of this policy and all other relevant policies within the business areas for which they are responsible
- Ensuring that all employees who report to them are made aware of and are instructed to comply with this policy and all other related policies
- Ensuring any risks arising from the use of the Council's IT resources are managed in accordance with the Corporate Risk Management Policy.
- Consulting with the Human Resources and Workforce Development in relation to appropriate procedures to follow when a breach of this policy has occurred
- Consulting with the Legal and Democratic Services and IT Services in relation to the appropriate actions to be taken when an actual or suspected breach of data security has occurred.

Users

Each user is responsible for:

- Complying with the terms of this policy and all other relevant policies, standards, procedures, regulations, and applicable legislation
- Completing all information and cyber security awareness training within the given timescales
- Respecting and protecting the privacy and confidentiality of the information they have access to at all times
- Reporting all suspected misuse and breaches of this policy to their line manager immediately. If it is not appropriate to raise with the line manager the Council has a Whistleblowing policy in place that can be used.
- Reporting all actual or suspected breaches of data security to their line manager, Legal and Democratic Services and IT Services immediately.

Logging and Monitoring

The Council reserves the right, consistent with the relevant legislation listed within the policy to exercise control over IT resources and to monitor their use to ensure efficient operation, to detect misuse and to supply evidence if required, for use in disciplinary, legal proceedings, as a response to Freedom of Information requests or any other matter as deemed appropriate and necessary.
By using any Council IT resource or by accessing any Council system users accept that all use may be monitored.

Breaches of Security

Any individual suspecting that there has been or is likely to be a breach of data security must inform their line manager who must inform Legal and Democratic Services, HR and IT Services immediately. They will advise the individual and their line manager on what action should be taken.
Users should also be aware that they can use the Council's whistleblowing procedures to raise a concern if the concern they want to raise presents a danger, risk, malpractice or wrongdoing which affects others .
The Council reserves the right to take such action as it deems appropriate should the terms of this policy, or any sub-policy, be breached. Any person found to have breached or attempted to breach this policy or any sub-policy may be subject to disciplinary action under the Council's Disciplinary Policy, up to and including summary dismissal.

Supporting Policies, Standards, Procedures and Guidelines

There are a number of supporting policies, standards, procedures and guidelines to accompany this IT Security Policy. All are published on the intranet

Review & Update

This policy will be reviewed and updated annually or more frequently, if necessary, to ensure that any changes to the Council's governance structure and business practices are properly reflected.

Policy Distribution & Awareness

This policy and all supporting policies, standards and guidelines will be issued via the Council's My Policies Application.

Users are required to acknowledge that have read and understand this policy and consent to adhere to the rules outlined therein.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Appendix A

Authorisation / Authorised: Official approval and permission to perform a particular task.

Availability: Ensuring that authorised users have access to information and associated assets whenever required.

Breach of Data Security: The situation where sensitive data has been put at risk of unauthorised disclosure as a result of cyber compromise, the loss or theft of the data or, the loss or theft of a computer or storage device containing a copy of the data or through the accidental or deliberate release of the data.

Confidentiality: Ensuring that information is only accessible to those users who are authorised to access the information.

Council Network: The data communication system that interconnects different wired and wireless Local Area Networks (LAN) and Wide Area Networks (WAN).

Cyber risk: Any risk of financial loss, disruption, or damage to the reputation of the organisation from some sort of failure of its information technology systems or those of its partners/third parties.

IT resources: Includes all computer facilities and devices, networks and data communications infrastructure, cloud resources, telecommunications systems and equipment, internet/intranet and email facilities, software, information systems and applications, account usernames and passwords.

Information: Any data in an electronic format that is capable of being processed or has already been processed.

Information Asset Owner: The individual responsible for information assets within their service area. This is generally the service director. …….

Information Asset Assistant: The individual nominated by the Information Assest Owner to assist the Information Asset Owner with their responsibilities as Information Asset Owner

Cyber Security: The protection of IT services and devices we all use (systems, servers, laptops, computers, tablets, printers, portable storage devices and smartphones), and the services we access from theft, loss or damage.

Information Security: The preservation of confidentiality, integrity and availability of information (whether verbal, paper based or online).

Information System: A computerised system or software application used to access, record, store, gather and process information.

Integrity: Ensuring the accuracy and completeness of information and associated processing methods.

Line manager: The individual a user reports directly to.

Process / Processed / Processing: Performing any manual or automated operation or set of operations on information including:

- Obtaining, recording or keeping the information

- Collecting, organising, storing, altering or adapting the information
- Retrieving, consulting or using the information
- Disclosing the information or data by transmitting, disseminating or otherwise making it available
- Aligning, combining, blocking, erasing or destroying the information.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Third Party Commercial Service Provider: Any individual or commercial company that have been contracted by the Council to provide goods and/or services to the Council.

Threat: A potential cause of an incident that may result in harm to a system or organisation.

Users: Any individual using any of the Council's I.T. resources.

Gateshead Council

Acceptable Use Policy

Introduction

IT resources, such as PCs, laptops, tablet devices and smart phones offer new and exciting ways of working and engaging with our colleagues and citizens. However, we must also be aware that improper use can impact us, our colleagues, citizens, the Council's reputation and the public purse.

In this policy the expressions "Council" or "Gateshead Council" includes any agents, third-party organisation or company that utilises Gateshead Councils IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Purpose

This Acceptable Use Policy aims to protect all users of the Council's IT resources and to minimise such risks by providing clarity on the behaviours required by Gateshead Council and its employees.

It sets a framework within which to conduct the Council's business and explains how we can achieve compliance with new business and technology requirements.

It also aims to ensure that all users understand their responsibility for the appropriate use of Gateshead Council's IT resources. Understanding this will help users to protect themselves and Gateshead Council's equipment, information and reputation.

Scope

This policy sits below the Council's overarching IT Security Policy and applies to all IT resources that stores or processes Council data.

For the purposes of this policy, IT resources can include but is not limited to user accounts, end-user devices, systems, applications, networks, cloud resources, printers, telephones and customer facing web services.

This policy is mandatory for all persons who have been granted access to any Council IT resource.

Definitions

A list of terms used through this policy are defined in within **Appendix A** of the overarching IT Security Policy.

Policy Statements

All users are required to adhere to the IT Security Policy and all sub-policies.

This policy is a sub policy to the Council's IT Security Policy.

General principles

Users will:

- Be responsible for their own actions and act responsibly and professionally, following the Gateshead Council Code of Conduct while respecting the Council and fellow employees, suppliers, partners and citizens.
- Use IT resources and the information they hold in line with Gateshead Council security and Information Management policies
- Ensure any risks arising from the use of the Council's IT resources are managed in accordance with the Corporate Risk Management Policy.
- Immediately report any breach of this Acceptable Use Policy to their line manager or Service Director who will then discuss the next steps with their nominated HR advisor.
- Be aware that they can use the Council's whistleblowing procedures to raise a concern if it is believed that someone is misusing council information or electronic equipment.
- Understand that both business and personal use of corporate IT resources will be monitored as appropriate.
- Undertake education and awareness on cyber security, including completing cyber security awareness modules via the Learning Hub in order to be able to understand, recognise, and report threats, risks and incidents.

Users will NOT:

- Undertake illegal activity, or any activity that could be harmful to Gateshead Council's reputation or jeopardise staff and/or citizen data, on any IT resource.

User IDs and passwords

Users will:

- Always protect usernames and passwords from disclosure.
- Create secure passwords following best practice guidance.
- Always lock the screen when temporarily leaving devices that are in use.
- Always log out of all devices connected to the council's network when not in use for a period of time.
- Immediately report any suspected breach or attempted breach of their account to the IT Service Desk.

Users will NOT:

- Share their passwords with anyone, including IT Services.
- Log on to any council system using another user's credentials.
- re-use of passwords across multiple applications and services.

Managing and protecting information

Users will:

- Understand that they must adhere to the Council's Data Protection Policy in order to protect Council information.
- Be careful not to be overheard or overlooked in public areas when conducting Council business.

- Comply with the Councils guidelines and procedures for managing all Council information.

Users will NOT:

- Attempt to access Council data unless there is a valid business need that is appropriate to their job role.
- Provide information in response to any request where the requesters identity cannot be verified.
- Attempt to access, amend, damage, delete or disseminate another persons files, emails, communications, or data without the appropriate authority.
- Attempt to compromise or gain unauthorised access to any Council IT resource or the content it holds, or prevent legitimate access to it.

Personal use of Council IT

Users will:

- Understand that they are personally accountable for what they do online and with any IT resource.
- Understand that personal use of IT resources is only permitted in an employee's own time, when not on official duty and 'Clocked out' as per the Flexitime Working Scheme. Breaks taken in normal working hours, such as paid breaks, do not count as the employee's own time for personal use of Council equipment.
- Understand that the ability to store personal information (data related to employees that is not related their job) is only permitted within their personal drives (Z:\ Drive or OneDrive), and that Gateshead Council has the right to require the data be removed should it interfere with business activity or use.
- Ensure activities do not damage the reputation of Gateshead Council, its employees or citizens. This includes accessing, storing, transmitting or distributing links to material that:
    - Could embarrass or compromise the council in any way.
    - Is obtained in violation of copyright or used in breach of a licence agreement.
    - Can be reasonably considered as harassment of, or insulting to, others.
    - Is offensive, indecent or obscene including abusive images and literature.

Users will NOT:

- Misuse their official position, for example by using information acquired in the course of official duties to further their private interests or those of others.
- Trade or canvass support for any organisation while working on official premises or from any Council issued IT resource, whether it is for personal gain or on behalf of external bodies.
- Send messages or material that solicit or promote religious, political or other non-business related causes, unless authorised by the council.
- Provide unauthorised views or commitments that could appear to be on behalf of the council.
- Undertake any form of gaming, lottery or, betting.
- Use any type of applications and/or devices to circumvent management or security controls.
- Download software onto council devices, with the exception of council supplied tablet devices and smart phones where permitted from an official source and appropriately

licensed. This software must not compromise the performance or security of the device.
- Download music, video or other media-related files for non-business purposes or store such files on network drives.
- Attempt to download any attachment or click on any links from any personal webmail accounts on any Council IT resource.

Email/fax/voice communication

Users will:

- Comply with the council's email policy at all times
- Only use appropriate language in messages, emails, faxes and recordings. Threatening, derogatory, abusive, indecent, obscene, racist, sexist or otherwise offensive content will not be tolerated
- Be vigilant to phishing emails and know how to spot and report suspicious emails.
- Only use your council email address for council business related activities and linked organisational activity (e.g. council discount schemes, Trade Union activity and other officially provided Internet links).
- Use their personal email address for personal activities including purchasing and selling of goods, internet banking and any other personal activity.

Users will NOT:

- Use their council email address for any personal use.
- Engage in mass transmission of unsolicited emails (SPAM).
- Alter the content of a third party's message when forwarding it unless authorised.
- Try to assume the identity of another user or create or send material designed to mislead people about who originated or authorised it (e.g. through misuse of scanned/digital signatures).

Websites and Social Media

Users will:

- Only access appropriate content when using council IT resources and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as described in the Web Filter guidance.
- Report any access to a site that should be blocked by our web filters to their line manager and to IT Services via the dedicated AssystNET form.
- Request a review following the online process for any website that is blocked but where a legitimate business need exists to access the site.
- Use social media appropriately by making themselves aware of the Council's Social Media Policy.
- Only use approved council social media accounts for official business and where appropriate, use council branding and a professional image or persona on such accounts.
- Be aware that their social media content may be available for anyone to see, indexed by Google and archived for posterity.

Users will NOT:

- Attempt to download any file types from any unknown or unreputable sources.

- Attempt to upload or store any council information on any none approved Cloud Service
- Input any council information including anything that is sensitive / personal information onto online forums, blogs or social networking sites.

Devices, systems and networks

Users will:

- Understand that the council permits only certain approved devices (such as managed Agile Devices) to connect to the Internet via WiFi or Ethernet. When doing so, the Remote Access Security Policy must be adhered to at all times.
- Understand that they are permitted to utilise personal hotspot (tethering) technologies via a council or personal mobile phone in order to wirelessly connect to the Internet for business purposes. However, please be aware that this may have incur additional charges.

Gateshead Council cannot be held liable for any additional data charges this may incur if tethering to a personal mobile device. Therefore, any use of a personal phone for this purpose is the individual's choice.

- Understand that all requests to use new software not currently approved by Gateshead Council must be subject to the Software Request process though AssystNET. Note that this is not required when installing applications onto Android or iOS devices.
    - Contact IT Services if travelling outside of the UK and wishing to take council devices with them. Council devices, including smart phones, must only be taken outside the UK when required for official business and approved by your line manager. Gateshead Council may prohibit the carrying and use of council devices in certain countries.

Users will NOT:

- Connect any mobile devices (business or personal) by USB cable to any Council IT resource for any purpose including uploading and downloading files or charging.
- Use any personal wallpapers or screensavers.
- Store any Council information on any devices or application where the council's security controls have not been applied.
- Connect any non-council issued device to any council network other than those specifically provided for personal use such as Guest WiFi.

Physical Security

Users will:

- Be responsible for keeping all portable devices assigned to them safe and secure and will:
- Immediately contact the Service Desk via telephone on 433 3771 to report any lost portable device.
- Immediately report any damage of their equipment to their line manager and to the IT Service Desk via the relevant AssystNET form.
- Protect council equipment appropriately when travelling e.g.laptops must always be carried as hand luggage.
- Never leave a portable device unattended in sight in parked vehicles or hotel rooms

- Do not leave council equipment in parked cars overnight
- Without delay, return all council equipment when leaving Gateshead Council. Line Managers must complete all appropriate exit procedures with leavers

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

Personnel Security Policy

Introduction

Personnel security is a system of policies, standards, procedures and technical measures, which combine to mitigate the corporate risk of legitimate access to Gateshead Council assets being exploited for unauthorised purposes. In particular, this policy serves to mitigate the “insider threat” and associated operational risks, the causes of which are inherent vulnerabilities arising from accidental, negligent or deliberate (malicious) actions by people working on the physical or IT estate.

In this policy the expressions “Council” or “Gateshead Council” includes any agents, third-party organisation or company that utilises Gateshead Councils IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Purpose

The purpose of this policy is to define the Council’s requirement for personnel security controls and how and where they should be applied, and in so doing mitigate the corporate risk of unauthorised access to Council data, IT resources and physical premises.

Scope

This policy sits below the Council’s IT Security Policy and applies to all IT resources that stores or processes Council data.

For the purposes of this policy, IT resources can include but is not limited to user accounts, end-user devices, systems, applications, networks, cloud resources, printers, telephones and customer facing web services.

This policy is mandatory for all persons who have been granted access to any Council IT resources.

Definitions

A list of terms used through this policy are defined in within **Appendix A** of the overarching IT Security Policy.

Policy Statements

All users are required to adhere to the IT Security Policy and all sub-policies.

This policy is a sub policy to the Council’s IT Security Policy.

The Council must ensure resources and processes are in place to deliver the requirements of this policy, in an integrated fashion where necessary, ensuring that dependencies are mapped and understood.

All individuals must comply at all times with procedures established under this policy.

Security awareness

To facilitate awareness and compliance the Council will maintain a Cyber Security awareness programme, the key principles of which are:

- all individuals must undergo IT induction upon commencement of their employment.
- all individuals must complete the annual Cyber Security E-Learning modules within the appropriate deadlines.
- all individuals should be made aware of and understand the contents and requirements of regular security awareness campaigns and communications, made available through all appropriate channels.
- all individuals can participate in the risk identification process, in accordance with the Council's corporate risk management arrangements.

Joiners, Movers and Leavers

To maintain best practice and support effective risk management, the Council shall ensure that simple procedures to enable all new starters - whether permanent or temporary staff or contracted resource - to have completed mandatory pre-employment checks (Baseline Personnel Security Standard) and to undertake the mandatory Cyber Security Awareness training upon entry to the Council and before they have access to any customer-facing systems or other sensitive data;

The Council shall ensure that it has IT systems, policies and simple and effective procedures in place to maintain a constant record of the numbers of individuals working on its physical or IT estate at all times, their usual work locations, and their working roles;

The Council shall ensure that it has policies, procedures, technical controls and monitoring capability in place and consistently implemented, such as to only allow those with specific access rights to operate on named IT systems and data sets: this is so as to provide assurance that access rights are being explicitly granted, rather than by default;

The movement of individuals between roles shall be understood and monitored to the extent that specific system, data and building access rights are granted in relation to a specific role and an individual's access needs relating to it;

Simple procedures shall be put in place, and monitored, such that anyone leaving the Council returns their IT equipment upon departure, and that access to IT systems, applications and data - wherever located - shall be removed at the same time;

All individuals and line managers must ensure compliance with the Joiners, Movers & Leavers Procedures and associated policies as defined.

Remote Working

Individuals who work remotely, or from home, including working from abroad, must ensure full agreement with their line managers and comply with the Council's Acceptable Use Policy, the Remote Working Security Policy and all other IT Security policies at all times.

Investigation and Disciplinary Measures

The Council shall put in place appropriate personnel policies and procedures to enable the timely investigation of any security incidents and/or allegations of internal fraud, contrary to the intentions of this policy.

The Council shall ensure that its personnel policies include effective and proportionate disciplinary measures, appropriately communicated to all individuals, such as to deter inappropriate behaviour under this policy.

Risk Identification

All employees are encouraged to be risk aware and to participate in the risk identification process. More information is available here: Corporate Risk Management Policy and Information (Gateshead Intranet)

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

Remote Working Security Policy

Introduction

For security purposes, remote working is identified as creating, accessing, processing, storing or handling Council information outside of the Council's network or business locations.

In this policy the expressions "Council" or "Gateshead Council" includes any agents, third-party organisation or company that utilises Gateshead Councils IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Purpose

The purpose of this policy is to define risk controls including preventative measures that protect and secure Council information and assets when working from remote locations, including from home, when travelling, when on third party premises and so on.

The policy addresses a number of operational risks (threats) to Council data, or implications related to its use:

Threat	Description
Device Loss	Devices used to access, transfer or transport work files could be lost or stolen.
Data Theft	Sensitive corporate data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware, and other threats could be introduced via devices.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the Council to the risk of non-compliance with various identity theft and privacy laws.
Excessive/inappropriate use of device	Excessive use of the device or use of Sim card when wi-fi is available will incur unnecessary costs for the council. Breakages and lost devices also incur a cost to the council.

The policy is designed to ensure that IT resources are used appropriately and do not incur any unnecessary cost for the council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Scope

This policy relates to the handling of any IT resource, all Council data (digital and paper based) including but not limited to:

- All types of computers e.g. Laptops\Desktops\MacBooks\Surface Pros
- Smart Devices e.g. Smartphones and Tablets
- Mobile Phones
- Digital cameras or recording devices
- Any other portable device, navigation system or a hybrid device that combines functionality

This policy applies to all Council employees and agents acting on their behalf (this includes students, temporary, casual, agency staff and volunteers working for or on behalf of the Council), who handle, process or store Council information remotely, and should be followed by individuals who:

- Work in remote environments on an ad hoc basis, e.g. mobile working within the community, in public areas, in hotels or using any public or private transport.
- Work from home with the appropriate approval and authorisation.

For the purposes of this policy;

- Managed Laptop refers to Council provided Dell Laptops
- Managed mobile device refers to a Council provided Apple tablet or phone or Android phone.
- BYOD refers to a device provided by the end user to access council systems and information i.e. Office 365
- Agile device refers to all of the above
- Citrix remote access refers to any device (both managed and BYOD) that provides access to the Council's Citrix infrastructure.
- Council paper records includes handwritten notes taking by Council officers during their working activities and any Council data printed into hard copy form

Definitions

A list of terms used through this policy are defined in within **Appendix A** of the overarching IT Security Policy.

Policy Statements

All users are required to adhere to the IT Security Policy and all sub-policies.

This policy is a sub policy to the Council's IT Security Policy.

General statements

All users must consider the sensitivity, classification and value of information being handled when working remotely and should understand the policy requirements on protecting Council information and assets, managing them accordingly, including:

- Only using systems, applications, software and devices which are approved by IT Services to undertake Council business.

- Consideration of classification and sensitivity of the information being worked on and whether it is appropriate to do so outside of a secure Council working environment.

- Not allowing any unauthorised persons to access IT resources or any Council information, including family members.

- Consideration of the sensitivity/classification of information and privacy requirements where smart devices/listening assistants are/may be present and active. This includes (but not limited to) Alexa, Siri, Google and Microsoft Cortana.

- Storing Council information and assets securely, ensuring also the appropriate secure destruction of Council printed information.

- Remaining vigilant when using Council information to reduce the risk of mishandling data which could lead to a security breach, particularly where remote working is in practice.

- Ensuring that any Council data that needs to be kept permanently is transferred onto an appropriate location i.e. on the corporate network or within the Council's Office 365 Tenant.

- Informing IT Services of any future plans to work remotely overseas.

When in transit, staff must not leave any IT resource or sensitive information (whether hardcopy or electronic) unattended at any time. If travelling by vehicle, IT equipment and Council information must be stored securely, out of sight and removed whenever the user leaves the vehicle.

Any lost or stolen device, managed or unmanaged, used to access and\or store Council information must be reported to the IT Service Desk immediately.

Users must immediately report to their manager and the IT Service Desk any incident or suspected incidents of unauthorised data access, data loss, and/or disclosure of Council information.

Shared Devices

For Council provide shared devices;

- Passcodes must be administered by a nominated departmental officer and all devices must be signed in and out whenever issued/taken by an employee.
- Council information must not be stored locally.
- Council systems/information can only be accessed via Citrix using the user's unique username, password and MFA login.

Use of unmanaged devices to conduct Council business

Where Council systems are configured to permit access from unmanaged devices, user are;

- Responsible for the confidentiality and integrity of all Council information held on their unmanaged device.
- Required to enable and configure encryption for any unmanaged device used to access and\or store Council information.

- Responsible for the removal of any Council information held on their unmanaged device in accordance with the Councils Retention Policy and if they leave their current post of employment.

The Council reserves the right to inspect any Agile device to ensure the security / deletion of Council information at any time, even after termination of employment with the Council.

Data Usage

SIM Card data must not be used for any personal use of IT resources when working remotely.

Users understand that data usage on SIM cards provided by Gateshead Council is monitored to record sites accessed, times, dates, duration of access and so on in order to identify unusual usage patterns or other suspicious activity.

Responsibilities

Line Managers are responsible for, and must ensure that:

- Employees are made aware of the relevant Security Policies and HR Policies which support working securely in remote locations.
- Equipment is appropriately authorised; Council assets are accounted for, and a record maintained prior to issue and use of all Council approved devices.
- Employees are made aware of the operational risks often associated with remote working and any additional service specific controls or procedures that must be followed. Examples of risks include:
    - the loss or theft of IT equipment or sensitive and personal data.
    - the inadvertent or deliberate disclosure of sensitive, operational information.
    - unsecured storage of information and user credentials, such as username and passwords.
    - tampering, where IT equipment/information is left unattended.

Users must always:

- seek line management approval, prior to undertaking any type of remote working, including hybrid working and travelling for official business outside of the UK, this list is not exhaustive.
- take personal responsibility to understand and comply with relevant Council security policies where circumstances are relevant.
- Be risk aware and raise any risks with management in accordance with the corporate risk management policy.

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

Email Policy

Purpose

This policy aims to help users understand what information can be sent using email and under what circumstances.

Whilst email may often appear to be an informal method of communication users should remember that it has the permanence of written communication, and as such users must ensure that it meets the same standards as other published documents.

In this policy the expressions “Council” or “Gateshead Council” includes any agents, third-party organisation or company that utilises Gateshead Councils IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Scope

This policy sits below the Council’s IT Security Policy and is mandatory for all persons who have been granted access to any Council email address.

Definitions

A list of terms used through this policy are defined in within **Appendix A** of the overarching IT Security Policy.

Policy Statements

All users are required to adhere to the IT Security Policy and all sub-policies.

This policy is a sub policy to the Council’s IT Security Policy.

When using email as a means of communication:

Users will:

- encrypt any email containing sensitive information by following the Council’s approved encryption procedures.

Users will not:

- Keep emails that are construed as business records in any email mailbox. Business records should be transferred to the appropriate corporate filing system as soon as possible
- Use council emails to conduct any business other than that of the Council.
- Use a Council email address to subscribe to websites accessed for personal use.
- Enter into any commitment on behalf of the Council unless explicitly authorised to do so.
- Generate emails in such a way that it appears to come from someone else.

- Send or forward email that could be construed as obscene, sexually explicit, racist, defamatory, abusive, harassing or which describes violent or criminal acts or otherwise represents values or opinions that are contrary to Council policy. Employees who receive email of this nature should inform their line manager immediately.
- Read, delete, copy or modify the contents of any other user's mailbox without prior authorisation in writing from a Service Director, unless access has been delegated to that mailbox by the mailbox owner.

ALL emails and attachments sent and received using a Council email address are owned by the Council.

Monitoring of email

IT Services make every effort to ensure the privacy of user data, including email messages. Any information obtained by IT Services during the course of systems administration will be treated as confidential and will not be used or disclosed in the normal course of events. Where routine systems management or administration indicates a breach of Council policy or the law, IT Services will bring this information to the attention of the Council or other relevant authorities.

Where there is reason to suspect misuse, management are able to access detailed reports of this information.

Users should note that all emails are potentially subject to disclosure under the Freedom of Information Act.

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

SMS and Instant Messaging Policy

Purpose

This policy aims to help users understand what information can be sent using SMS and instant Messaging (IM), this also includes chat messaging facilities built into some websites and applications when using a Council device or network.

The policy does not overrule any data protection legislation concerning the sharing of confidential, personal or sensitive data.

Whilst SMS/IM may often appear to be an informal method of communication users should remember that it has the permanence of written communication, and as such users must ensure that it meets the same standards as other published documents.

Note: This policy does not apply to emails, which are subject to their own policy.

Scope

The Policy applies to all Council employees and its representatives when using a Council device or the Councils network, including:

- Councillors
- Employees
- Agency staff
- Contractors
- Consultants
- Suppliers
- Service users
- Employees and committee members of organisations funded by Gateshead Council
- Employees and Principals of Partner Organisations

Definitions

A list of terms used through this policy are defined within **Appendix A** of the overarching IT Security Policy.

Policy Statements

- The use of SMS/IM is appropriate when it is being used to give routine non-personal business information and reminders.

- Due to the difficulty in ensuring the recipient is entitled to any requested information, SMS/IM must not be used for any exchange of any personal or sensitive data which includes (but is not limited to) date of birth, bank account details, addresses, benefit details, payroll data, information on family members and health/medical information.

- SMS/IM should not be used as a substitute for email. SMS/IM should be used only for questions or announcements that are short and need to be communicated immediately.

- Limited private use of SMS/IM when using the Councils network or devices, is permitted.

- Only approved applications and services should be used to send Council business SMS/IM.

- All SMS/IM messaging application must be configured in such a way to allow the auditing of all SMS and IM messages. At a minimum, this must include, the source user, the recipient(s), the time sent and an indication of the content of the message. SMS/IM messages are subject to FOI / SAR requests and must be stored in accordance with the Councils Retention Policy.

- All SMS/IM messages which are sent via the Council's managed devices and services are recorded and remain the property of the Council.

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

Information Classification Policy

Introduction

Information Classification is the process for classifying information into relevant sensitivity categories.

In this policy the expressions “Council” or “Gateshead Council” includes any agents, third-party organisation or company that utilises Gateshead Councils IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

Purpose

This policy describes the way that the Council has decided to protect its information, and when to apply markings if required.

This policy describes how Gateshead Council classifies information assets to: ensure they are appropriately protected; support Council business and the effective exploitation of information.

Scope

This policy sits below the Council’s IT Security Policy and applies to all IT resources that stores or processes Council data.

The policy applies to all information that the Council collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanged with external partners.
For the purposes of this policy, IT resources can include but is not limited to user accounts, end-user devices, systems, applications, networks, cloud resources, printers, telephones and customer facing web services.

This policy is mandatory for all persons who have been granted access to any Council IT resources.

Policy Statements

All Council information must be classified according to the following scheme to ensure that all persons know what level of security should be applied.

Personally Identifiable - Information that can be used to identify living individuals. These documents are likely to be bound by the requirements of the Data Protection Act.
Organisationally Sensitive - This classification includes any information relating to activity that does not identify living individuals but may cause operational difficulties if the information became corrupted, compromised, unavailable or disclosed.

Public Information - Information that does not identify individuals or include organisationally sensitive information and has not been published. This information may be subject to access requests under the Freedom of Information Act.

Published information - Information that has been published, including classes of information identified in the Council’s Freedom of Information Act publication scheme.

All Council systems and applications must be classified depending on the classification of data they store and\or process.

All emails, either automated or user generated, must be encrypted if they contain Personally Identifiable or Organisationally Sensitive information.

Personally Identifiable and Organisationally Sensitive information must not be shared over insecure channels.

Personally Identifiable and Organisationally Sensitive information must not be shared with any unauthorised parties.

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.

Gateshead Council

IT Asset Management Policy

Introduction

This IT asset management policy provides a framework for the appropriate and effective management of IT equipment (hardware and software), from procurement to disposal, in Gateshead Council.

It defines responsibilities that relate to the implementation of this policy and is designed to ensure that IT assets are:

- Managed appropriately from the point of acquisition to the time of disposal in a way that is compliant with the Council's policies and regulatory obligations;
- Procured correctly in line with the Council's strategic plans;
- Registered within the IT Service's asset management system for tracking and auditing purposes;
- Supported and maintained throughout their lifecycle so that they deliver best value for the investment;
- Controlled effectively to protect the data and information that they store or transmit; and
- Administrated in a way that enables the identification of risk and ensures business continuity.

This policy does not stand in isolation and must be implemented in conjunction with the wider range of information security, procurement and financial related policies of the Council.

Purpose

This policy is produced in response to the operational risk associated with IT assets and aims to provide a clear instruction on the appropriate management of physical IT assets to help to ensure that the Council is meeting its legal, regulatory, contractual and licencing obligations.

In this policy the expressions "Council" or "Gateshead Council" includes any agents, third-party organisation or company that utilises Gateshead Council's IT infrastructure and solutions (e.g. Schools, Regent Funeral Service) or accesses and utilises information held by Gateshead Council.

This policy does not replace any legal or regulatory requirements, to which all Council employees and suppliers must comply.

Scope

This policy applies to all physical IT assets purchased by or on behalf of Gateshead Council.

A physical IT asset is defined as:

- All desktop and laptop computers (including docking stations);
- All monitors, printers, scanners and portable storage devices;
- All phones and mobile data devices (e.g. smartphones, tablets and other portable computing equipment);

- All meeting and public area IT equipment;
- System software, client applications and associated licences;
- IOT Devices such as sensors, meters and any device that collects or stores data
- Any other IT peripheral provided by the council.

This policy also applies to all IT equipment that forms part of the Council's IT infrastructure (servers, routers, firewalls, switches, access points and other network infrastructure etc.) and any equipment that electronically stores data on the Council's central file storage systems or transmits it across the network.

This policy applies to all employees and other agents of the Council, including agency staff, contractors, partner organisations, suppliers and customers, who request or hold IT equipment
purchased by or on behalf of the Council.

Information asset management will be covered by a separate policy, in accordance with the requirements of the General Data Protection Regulation.

Definitions

A list of terms used through this policy are defined in within **Appendix A** of the overarching IT Security Policy.

Policy Statements

- The procurement of IT assets must be undertaken in consultation with and carried out by IT Services from inception. IT Services is responsible for engaging with the Council's Procurement Team and ensuring that the best procurement practice is followed as per the Council's policies and applicable legislation.

- Requests for individual IT assets must be submitted to IT Service via AssystNET or the IT Service Desk in accordance with current ordering processes and procedures.

- IT Services will assess requests for new and replacement IT equipment and, where possible, will fulfil them using existing equipment held within the centralised store.

- Requests for non-standard specialist IT equipment will be assessed by IT Services and approved via a business case through the appropriate channels, Total cost of the assets will be added to IT Services budget if the purchase is authorised by the relevant Service Director/Business Partner.

- For compatibility and efficiency reasons, IT assets will be issued on a 'fit for purpose' basis based on user roles and requirements.

- IT Services will not, without adequate justification, approve or proceed with the procurement of IT assets that do not comply with the requirements of the Council's plans, policies and standards.

- All IT equipment purchased by the Council will be stored in centralised asset management stores managed by IT Services when they have not been issued or are not in use.

- On behalf of the Council and in consultation with the Procurement Team, IT Services is responsible for identifying and managing sources and channels for the purchase of IT assets, utilising existing framework agreements whenever possible.

- All IT assets purchased by the Council are the property of Gateshead Council and will be deployed and utilised in a way that is deemed most effective for addressing the Council's needs and objectively demonstrates value for money. The budget for IT assets will be centralised and managed by the Resource and Digital Directorate on behalf of the Council, with the exception of Traded Services and Grant Funded equipment where separate arrangements apply.

- All IT assets purchased (excluding consumable items) will be registered in the asset management system and be asset tagged before being issued or put into use.

- The asset management system will be maintained by IT Services, to enable assets to be tracked, managed and audited throughout their entire lifecycle.

- IT assets will be appropriately administered and maintained to ensure they remain secure, fit for purpose and compliant with the licenced conditions of use during their entire lifecycle.

- End users are not allowed to install software on devices, unless authorised to do so. Requests should be made to the IT Service Desk to have additional software installed on to a device. Only approved software is permitted to be installed.

- End users must always contact the IT Service Desk if they need to move, reassign or return IT equipment.

- All IT assets that are no longer in use must be returned to the Council via the IT Service Desk for redeployment. This includes where the asset was purchased using specific service-related funds.

- In order to ensure the confidentiality of information, any IT asset that has been used to process or store personal or sensitive information will be 'wiped' by IT Services before being reissued and must go through a physical disposal and destruction process at the end of its useful life as defined by the IT Asset Disposal Policy.

- The management of IT assets must comply with this policy. Breach of this policy may result in any device being remotely wiped, blocked from the Council's network and being prevented from using Council provided services and software. A breach may also be considered a disciplinary offence.

Responsibilities

The IT Service Director is accountable for the implementation of this policy in the Council and on a day-to-day basis the IT Service will be responsible for:

- Coordinating IT asset audit activity such as annual inventory checks for management reporting;
- Updating and maintaining the accuracy of the asset management system as soon as a change is made (including office moves, reports of lost or stolen equipment and disposals);
- Ensuring that equipment is signed for by end users when collected from or returned to the IT Service and is recorded in the asset management system;

- Ensuring that all IT assets are processed, and asset tagged before they are issued to end users or entered into the central store;
- Checking equipment is returned in the same configuration as expected;
- Administrating the control and security of equipment held in stock for issuing and awaiting reissue or disposal;
- Ensuring that any IT asset that is retired is disposed of according to the IT Asset Disposal Policy;
- Ensuring that the relevant risk and control records are kept up to date;
- Giving correct and appropriate advice to users on the correct handling of IT assets; and
- Reporting any incorrect disposal or misuse of an IT asset to an appropriate manager within the IT Service as soon as possible.

End users issued with IT equipment will be responsible for:

- Retaining responsibility for equipment issued to them until it has been returned to the IT Service for redeployment or disposal;
- Ensuring that IT equipment is not moved to another location (if fixed) or transferred to another person without the consent of the IT Service;
- Reporting the loss or theft of IT equipment immediately to the IT Manager via the IT Service Desk or the Council Security Team;
- Reporting any defects and returning equipment immediately that is not operating normally to the IT Service via the IT Service Desk; and
- Returning all IT equipment to the IT Service upon replacement, when it is no longer required for Council business or when the holder leaves the Council.
- Raising any risks relating to the IT equipment in accordance with the Corporate Risk Management Policy.

Compliance

Line managers are responsible for ensuring that users understand their own responsibilities as defined in this policy and continue to meet the policy requirements for the duration of employment with the Council. It is a line manager's responsibility to take appropriate action where individuals fail to comply with this policy.

All Council employees are responsible for ensuring that they understand and comply with the security requirements defined in this policy and all other security policies. If for any reason, users are unable to comply with the policy, this should be discussed with their line manager in the first instance for resolution.

Non-Compliance

Any attempt to contravene or bypass any security measure documented within this policy, technical or written, will be deemed an intrusion attempt or a breach of security and will be dealt with in accordance with Gateshead Council's overarching IT Security Policy.

Policy Acceptance

Individuals requiring clarification on any aspect of the policy or any supporting policies, standards and guidelines and/or advice on general IT security matters should log a call via the dedicated AssystNET form.

By clicking Accept, employees acknowledge that have read and understand the above policy and consent to adhere to the rules outlined therein.