ICT Policy

Contents

1. Introduction 1
2. Executive Summary 1
3. Purpose of the Policy 1
4. Scope 1
5. Acceptable Use of ICT Resources 2
6. Working Practices – Office, Hot Desking, and Remote Use 2
7. Equipment and Software Controls 2
8. Data Protection and Privacy 3
9. Email and Messaging 3
10. Use of the Internet 3
11. Social Media and Networking 4
12. Passwords and Access Control 4
13. Backup and Data Recovery 4
14. Incident Reporting and Security Breaches 5
15. Staff Training and Assertion 10 5
16. Misuse of ICT Systems 5
17. Monitoring and Compliance 5
18. Policy Review 6
19. Conclusion 6

Issue Number	Date	Details of amendment
1	28.08.25	New policy – ICT Policy & Use of Computers etc merged

1. Introduction

1.1 East Grinstead Town Council recognises that Information and Communication Technology (ICT) plays a vital role in delivering efficient and effective services to the community. ICT enhances communication, record keeping, and public engagement, but it also introduces risks related to data protection, cybersecurity, and reputational damage. This policy combines and updates existing ICT and communications policies into one comprehensive framework, aligned with the NALC Practitioners' Guide 2025.

2. Executive Summary

2.1 This policy governs how staff, councillors, contractors, and volunteers use Council ICT systems, including email, internet, and social media. It promotes secure, responsible, and lawful use of digital resources, ensures compliance with legislation, and protects Council reputation, assets, and data integrity. It also meets the requirements of the 2025 NALC Practitioners' Guide, including the mandatory use of Council-owned email domains and compliance with Assertion 10: Data Compliance.

3. Purpose of the Policy

3.1 Promote lawful, secure, and efficient ICT use.

3.2 Protect Council assets from cyber threats, misuse, and data loss.

3.3 Ensure compliance with the UK GDPR, Data Protection Act 2018, Equality Act 2010, and related legislation.

3.4 Ensure compliance with the NALC Practitioners' Guide 2025, including the explicit requirements for Council-owned email domains and Assertion 10.

3.5 Provide clear standards for ICT, email, internet, and social media use.

3.6 Support operational continuity and public trust in Council services.

4. Scope

4.1 Applies to:

- All Council staff, councillors, contractors, volunteers, and authorised users.
- All Council-issued ICT equipment and services (computers, laptops, tablets, phones, cloud systems, networks, email accounts, and social media accounts).
- All Council-related activities carried out in offices, remotely, or via hot desking.

4.2 Personal devices must not be used for Council business. All official work must be conducted using Council-issued equipment.

5. Acceptable Use of ICT Resources

5.1 ICT resources are provided for Council business.

5.2 Limited personal use may be permitted if it does not impact security, productivity, or reputation.

5.3 Prohibited uses include:

- Downloading or distributing offensive, discriminatory, or unlawful material.
- Harassment, bullying, or abuse.
- Political or commercial activities unrelated to Council work.
- Circumventing security, hacking, or installing unauthorised software.
- Gambling or playing electronic games.

6. Working Practices – Office, Hot Desking, and Remote Use

6.1 Devices must be shut down daily and locked when unattended.

6.2 Files must be saved only to approved Council storage (e.g., OneDrive, SharePoint).

6.3 Devices must never be left unsecured in shared/public areas.

6.4 Remote workers must use Council laptops, secure Wi-Fi, and keep devices in safe locations.

7. Equipment and Software Controls

7.1 Only Council-approved software (managed by Wessex IT) may be installed.

7.2 Updates, licences, and patches are managed centrally.

7.3 Faults or issues must be reported immediately to Wessex IT via the Clerk.

7.4 USBs or external drives require prior authorisation.

8. Data Protection and Privacy

8.1 The Council complies with the six principles of data protection: lawfulness, fairness, transparency, purpose limitation, minimisation, accuracy, storage limitation, and security.

8.2 Requirements:

- Collect/store only necessary data.
- Use encrypted cloud storage.
- Share data only with authorised parties.
- Follow retention and disposal schedules.
- Prevent unauthorised processing or disclosure.
- Comply with Assertion 10: Data Compliance under the NALC Practitioners' Guide 2025.

9. Email and Messaging

9.1 All Council business must use @eastgrinstead.gov.uk addresses or another Council-owned domain as required by the 2025 Practitioners' Guide.

9.2 Emails must be professional, respectful, and checked before sending.

9.3 Emails are subject to Freedom of Information (FOI) disclosure.

9.4 Councillors must not send contractual or binding instructions—officers only may do so.

9.5 Email accounts may be accessed by the Council in prolonged absences.

9.6 Inappropriate or excessive personal use is prohibited.

9.7 Messages via text must be clear, professional, and Council-related.

10. Use of the Internet

10.1 Internet access is primarily for work purposes. Limited personal use is acceptable only in exceptional circumstances.

10.2 Prohibited activities include:

- Accessing or distributing offensive, pornographic, or unlawful material.
- Fraud, piracy, hacking, or malware distribution.

- Sharing confidential information without authorisation.
- Misrepresenting personal opinions as Council views.

10.3 The Council may monitor internet usage and block inappropriate sites.

11. Social Media and Networking

11.1 Only authorised officers may post on official Council accounts.

11.2 Personal use of social media must not bring the Council into disrepute.

11.3 Councillors should keep personal and Council roles separate.

11.4 Users must not:

- Make derogatory, discriminatory, or defamatory comments about the Council, members, staff, or the public.
- Use Council email addresses for personal accounts.
- Disclose confidential or sensitive information.

11.5 Staff and councillors are personally responsible for published content. Breaches may result in disciplinary or legal action.

11.6 This section aligns with NALC Social Media Policy Guidelines (2024).

12. Passwords and Access Control

12.1 Strong, unique passwords must be used for all accounts.

12.2 Passwords must not be shared.

12.3 Two-factor authentication (2FA) must be enabled where possible.

12.4 Passwords should be changed regularly and kept confidential.

12.5 Access is on a need-to-know basis only.

13. Backup and Data Recovery

13.1 Data is backed up automatically by Council IT systems.

13.2 Users must not create their own backup copies.

13.3 Data recovery is managed by Wessex IT in line with Council protocol.

14. Incident Reporting and Security Breaches

14.1 All ICT issues or suspected breaches must be reported immediately to the Clerk or Wessex IT.

14.2 Incidents will be investigated and, where necessary, reported to the ICO.

15. Staff Training and Assertion 10

15.1 Mandatory annual ICT and data security training covers:

- Data protection and confidentiality.
- Recognising phishing and scams.
- Safe cloud storage and remote use.
- Equality and respectful communication.

15.2 Training supports Assertion 10: Data Compliance as defined in the NALC Practitioners' Guide 2025.

16. Misuse of ICT Systems

16.1 Examples include:

- Accessing another user's account.
- Downloading malware or prohibited content.
- Using Council systems for bullying or harassment.
- Leaving devices unsecured in public.
- Wasting ICT resources.
- Ignoring Council protocols.

16.2 Misuse may lead to disciplinary action or legal referral.

17. Monitoring and Compliance

17.1 The Council reserves the right to monitor ICT, email, internet, and social media use.

17.2 Monitoring will be lawful, proportionate, and GDPR-compliant.

17.3 Email and internet use may be audited for productivity, misconduct, or system security.

18. Policy Review

18.1 This policy will be reviewed annually or when legislation/technology changes.

18.2 Updates will be shared with all users, who must confirm understanding.

18.3 Reviews will ensure continued compliance with the NALC Practitioners' Guide 2025.

19. Conclusion

19.1 By following this policy, users ensure the responsible, lawful, and secure use of ICT, email, internet, and social media in support of East Grinstead Town Council's services and reputation, while meeting the requirements of national legislation and NALC guidance.

Adoption date: 13th January 2026
Reviewed: January 2028