Corporate Acceptable Use Policy

Hampshire County Council

Document Type	Policy
Title	Corporate Acceptable Use Policy
Document Owner	Simon Williams & Peter Andrews
Last revision date	29 September 2026
Version	3.61
Document status	Approved

Table of Contents

1. Introduction 2
2. Policy principle 2
3. Policy statements 2
4. Misuse definition 4
5. Personal use 5
6. User supplied IT equipment applications and services 6
7. Phishing e-mails 6
8. Social media 7
9. Artifical intelligence (AI) services 7
10. Reporting losses 7
11. Policy misuse 7
12. Monitoring 7
13. Investigations and information requests 8
14. Non-compliance 8
15. Policy review 8
16. Appendix A 9

Further reading 9

Relevant legislation 9

17. Document control 9

Corporate Acceptable Use Policy

Hampshire County Council

1. INTRODUCTION

This document sets out the overarching principle and subsequent policy statements for the expected use of Council supplied information systems (for example, cloud based and locally hosted systems) and IT equipment (for example, Laptops, PCs, mobile phones, and tablets) from any location.

This policy applies to all Hampshire County Council employees, County Councillors, agency workers, external contractors, partner organisation employees, consultants and voluntary workers, collectively referred to as **"users"**. It also applies to any third parties who have access to HCC information, information systems or services.

2. POLICY PRINCIPLE

All users of Council supplied information systems and IT equipment are required to operate them for their intended work purpose, in a lawful, secure, and responsible manner, knowing that their use may be monitored in accordance with Council policy.

3. POLICY STATEMENTS

All users of Council supplied computer systems and IT equipment are, therefore, required to adhere to the following statements:

- Users must complete the Corporate Acceptable Use Policy eLearning course upon recruitment and then at least annually (this includes reading and accepting the Corporate Acceptable Policy, this document).
- Users must use Council systems including internet access, email facilities, mobile devices, and IT equipment for their intended work purposes. This use of Council systems must:
  - be legal.
  - not prevent the Council from meeting its legal obligations including, but not limited to, the UK (United Kingdom) General Data Protection Regulation (GDPR)
  - not constitute misuse, as defined in section 4.
- Users must ensure that information which is confidential to the Council is not used or disclosed to others, for your own purposes, or any other purposes, information concerning the business of the Council.
- Users must ensure Council information is always secure and appropriately safeguarded in line with the Corporate Safe Information Handling Policy.
- Users must only use approved methods to access Council systems in HCC offices and remotely.
- Users must use passwords and other authentication methods that comply with the corporate password policy and must not ever disclose or share passwords.

- Users should ensure that credentials used to join networks or internet are removed (forgotten) when using a shared or pool device.
- Users must understand they are responsible for:
  - the actions performed under their allocated Council user identity (user ID) for example, userid@hants.gov.uk and must not allow another person to use their user ID.
  - all devices providing access to Council information that they use and must ensure these devices are secure when left unattended.
  - Users must not use technology or devices, (e.g. Mouse Wigglers etc.) which prevents or delays their device screen from locking.
  - reporting any loss of Council information or device containing Council information as soon as they are aware of the loss.
- Users must not install unauthorised software. Only software from IT-approved app stores can be installed by users.
- Users should avoid the use of Mass Storage Devices, MSDs (for example, USB sticks, SD memory cards or portable hard disks) wherever possible and instead use corporately provided services. Where this is not possible:
  - Users must seek approval from their Departmental SIRO (Senior Information Risk Owner) to enable MSD access on their device.
  - No personal data or HCC internal information can be stored on MSDs unless it is protected using at least 256-bit AES (Advanced Encryption Standard) encryption and only then with permission of the manager who is responsible for the data.
  - Users must be confident that the MSD is free from viruses and malware.
  - The data must be deleted from the MSD as soon as it is no longer required.
  - Care must be taken to avoid the loss of the device. Any losses must be reported immediately.
  - Information stored on MSD that needs to be available after the MSD's lifetime (as defined by the manufacturer) should be transferred to a corporately approved IT service to avoid information loss.
- Users should use the corporately provided secure printing service. Users should not print personal or sensitive HCC data when working remotely, however where this is unavoidable, the corporate Safe Information Handling Policy should be followed.
- Users must not store payment card data in any format outside of approved, PCI-certified services or locations.
- Users must not send payment card (for example, credit or debit card) details using electronic messaging systems (For example e-mail, instant messaging, SMS, chat).

- Users are aware that monitoring tools are in place and monitoring takes place. This monitoring by the Council is undertaken to ensure policy compliance and shall be in accordance with the IT and Digital Services Monitoring Policy.
- Users must assist with investigations into suspected breaches of this policy and understand that where non-compliance with this policy has taken place, appropriate disciplinary action including dismissal may be taken (see sections 9 through 12).
- Users must seek approval from their Line Manager and Assistant Director / Director before using HCC IT equipment or services from outside of the UK and European region. This approval can only be granted for a short-term, temporary period and is limited to maximum of six weeks in one UK financial year.
- Users must not use TikTok on Council supplied devices unless it is essential for their role and approved by the Communications and Engagement Steering Group (via the Head of Policy and Public Affairs).
- If asked to take a reasonable action by IT (for example, “Please change your password”) users must do so within 10 working days.
- Televisions and other screens must not be used to show films, television programs, and other audiovisual content for which copyright licences may be required. To avoid this, screens must only be used to view the BBC News Channel, Sky News, BBC Parliament and / or content owned by Hampshire County Council. They must not be switched over to other channels and measures must also be in place to prevent such channel changing.
- Council supplied computer systems and IT equipment must not be used to view films, television programs, and other audiovisual content for which copyright licences are required. These are not in place for your devices and if you view such content, then you risk infringing copyright.

4. MISUSE DEFINITION

It is prohibited to use your user ID or Council computer systems, such as internet access and email facilities:

- for the creation, use, transmission, or encouragement of material which:
  - is illegal, obscene, libellous (defamatory)
  - is related to the promotion of violent or unlawful extremism or terrorism ideology
  - is offensive, threatening, harassing or discriminatory
  - infringes another person’s copyright
  - transmits unsolicited commercial or advertising material
  - for illegal activities including, but not limited to, breaching the UK GDPR; Data Protection Act 2018; Computer Misuse; Obscene Publications and Design Copyright & Patents Acts

  - for activities which bring the Council's reputation into disrepute
  - for obtaining unauthorised access to the Council's, or another organisation, IT facilities
  - for violating or otherwise intruding upon other people's privacy
  - to wilfully disrupt other users' work in any way, including with viruses or by corrupting information
- for unauthorised downloading of copyrighted or confidential information
- to waste network and staff resources
- to express personal views which could be misinterpreted as those of the Council, or which are prejudicial to the interests of the Council
- for storing any payment data (for example, credit or debit card details) in any electronic Council systems or electronic messaging services
- to commit the Council to purchasing or acquiring goods or services without proper authorisation.
- to use TikTok on Council supplied devices unless it is essential for your role and approved by the Communications and Engagement Steering Group (via the Head of Communications and Engagement)
- if you fail to take a reasonable action within 10 working days, when requested by IT (for example, "Please change your password")

The misuse of internet access as described here applies regardless of which IT element is provided by the Council.

5. PERSONAL USE

Users may use Council supplied systems and devices including email facilities and internet access, for occasional personal use at the discretion of their manager, provided the activities do not constitute misuse or impacts on the user's work.

Users are also permitted to make reasonable use of the Council supplied equipment for personal requirements. However, it should be noted that:

- Council and personal emails should remain segregated (which they are when using MS Office mobile application).
- The storage of personal data (such as photographs or documents) is permitted but must not impact the intended work purpose of the device.
- The security of the user's personal data (for example, when used in online transactions) on Council supplied equipment is the responsibility of the user, not the Council.
- The provision of corporate telephony, specifically Teams external calling capability and corporate mobile phones, is exclusively for business calls. Personal use is strictly prohibited.

- It is the employee's responsibility to remove any personal information from a County Council issued device before they leave their employment, at which time the device will be wiped, and any information deleted.
- The Council cannot be held responsible for any loss of data in the case of automatic deletion (e.g., by anti-virus protection or when the device is returned at the end of employment).
- It is the employee's responsibility to return all IT equipment via their Line Manager when they leave employment. Failure to do so could result in commencement of the IT Equipment Recovery Process.
- The back-up and recovery of personal data stored on Council supplied equipment is the responsibility of the user, not the Council.

6. USER SUPPLIED IT EQUIPMENT APPLICATIONS AND SERVICES

The user's role may allow them to use their own IT equipment to access Council systems. These devices, such as PCs, Laptops, Tablets and Smartphones may connect to the corporate wireless (Wi-Fi) networks, where it is available and are permitted to access to Council systems provided:

- The user does not store or process any Council information (including personal data as defined by the GPDR) outside of the corporately approved applications and services without appropriate assessment, permission, and protection.
- The devices are not physically connected to the corporate wired network in HCC buildings.
- Only approved methods of remote access are used to access Council systems.
- These devices are not used to access special category personal data, the Public Services Network (PSN) or Council systems that hold PSN data.
- The software used to access Council systems and Council information is deleted from the device if the user's role no longer requires that they use their own devices to access Council systems, and at the end of the device's useful life.
- All software is regularly updated and is still in support with the vendor.

7. PHISHING E-MAILS

Users must demonstrate security awareness and specifically recognise phishing attacks, taking appropriate action to report phishing e-mails.

Phishing simulations are undertaken by the Council, and users must not click links or enter their credentials. Users are required to take the training available if they do click links and/or enter credentials.

The Council reviews phishing simulation results. Employees that repeatedly fail to demonstrate security awareness may be provided support under the Council's Managing Performance policy. In some circumstances action may be taken under the council's Managing Misconduct policy.

8. SOCIAL MEDIA

Users can participate in social media activities for the Council if the use is in accordance with and their manager's instruction, the Social Media Policy and the use of social media is part of their role's intended work purpose.

Note: Additional policy controls are in place regarding the use of TikTok on Council supplied devices (see Sections 3 and 4 for details).

9. ARTIFICAL INTELLIGENCE (AI) SERVICES

Users must not give access to Artificial Intelligence (AI) tools. Any requests for AI based services must go through the Application Request process. This includes, but is not limited to, granting permissions to cloud AI services accessed from your browser.

Refer to the Artificial Intelligence Policy for further information.

10. REPORTING LOSSES

Users must report immediately to the IT Service desk any loss of:

- Council information
- Any Council device
- Any personal device containing Council information.

If any information is at risk this must be stated at the time of reporting the loss, so the Information Governance team can be informed. This will enable the Information Commissioner to be informed if it is appropriate.

11. POLICY MISUSE

Users are expected to report suspected misuse of this policy, whether accidental or deliberate. Even if an event is not considered serious, it should be reported as it may be part of a wider issue or trend.

12. MONITORING

Users must be aware that:

- monitoring and reporting of their usage may be undertaken by the Council to ensure compliance to this policy.

- the Council's use of monitoring tools will be in accordance with the IT and Digital Services Monitoring Policy
- any communications sent or received by means of the Public Service Network (PSN) may be intercepted or monitored.

13. INVESTIGATIONS AND INFORMATION REQUESTS

Users are:

- expected to assist with investigations into suspected breaches of this policy conducted by police, internal audit, IT or HR.
- required to help the Council's Information Governance Team in response to statutory requests (for example, Freedom of Information (FOI) requests, UK GDPR requests).

14. NON-COMPLIANCE

To prevent non-compliance, users are encouraged to refer to online versions of this policy to ensure they remain up to date with any changes that occur.

Non-compliance with this policy or any misuse, including users spending what their manager considers excessive time on personal use, may result in access and computer equipment being withdrawn and/or disciplinary action. In the case of Council employees this disciplinary action could lead to dismissal.

The correct course of action, including consulting the police, will be determined after seeking advice from Human Resources, Information Governance and Legal Services.

Where misuse presents a safeguarding concern, the Local Authority Designated Officer or Adult Safeguarding team will be contacted.

15. POLICY REVIEW

This policy will be reviewed by the Document Owner on an ongoing basis. This policy will have at least an annual policy review governed by the Information Security Management Forum to an agreed schedule.

16. APPENDIX A

Further reading

Corporate Acceptable Use Policy e-learning	Data Protection (GDPR) e-learning
Mobile Messaging App Usage at Work Policy	Social Media Policy
IT and Digital Services Monitoring Policy	Safe Information Handling Policy
User ID and password guidance	Information Governance Policies
Artificial Intelligence Policy	

Relevant legislation

General Data Protection Regulation (GDPR)	Freedom of Information 2000
Data Protection Act 2018 (DPA)	Regulation of Investigatory Powers Act 2000
Computer Misuse Act 1990	Copyright, Design and Patents Act 1998

17. DOCUMENT CONTROL

Version	Change date	Changed by	Brief Description
1.0	04.2012	GCS	Combined conditions of use and Acceptable use statements Previous version 1.1 (2014); 1.2 (03.2015) 1.3 (11.2015)
1.4	11.2015	DW (David Wigley)	Amended the requirement for periodic password changes on the Good app. Added an item under password misuse for easy to guess passwords.
1.5	01.2016	JC	As a result of Internal Audit – Password management software is not used.
1.5.1	08.2016	GCS	Added statement emailing payment card details is not permitted. Password management software may be used in line with Password policy. Removed two download statements.
1.5.2	09.2016	GCS	Updated references errors in section 1.3.1
1.7	06.2017	GCS	Split away guidance material.
1.8	10.2017	JC	Moved line ‘for activities which bring the Council’s reputation into disrepute’ up in the priority and added the word ‘userid’ to this ‘It is prohibited to use your Council userid or Council supplied computer systems, such as internet access and email facilities:’
1.9	05.2018	GCS	Added reference to EPP (Enabling Productivity Programme) devices. Spacing changes. GDPR updates.

Corporate Acceptable Use Policy

Hampshire County Council

Version	Change date	Changed by	Brief Description
1.10	07.2019	MW	Annual review.
1.11	08.2020	Gilly Cruse-Small/ David Wigley / Colin McManus/ Holly Appleby-Scriven	Annual review implementing changes requested by DW and E Gilbert. The **Mass Storage Policy** and the **Remote Access Policy** have been absorbed into Section 1.3 of this policy. Updated Ownership of document & Governance
2.0	11.2021	David Wigley	Updated 1.1 to remove references to the guidance document. 1.3, 1.4 and 1.10 Replaced GDPR with UK GDPR 1.3 Updated the security incident reporting link Updated 1.3 with the following: • Requirement to complete annual AUP (Acceptable Use Policy) eLearning course. • Requirement to obtain Departmental SIRO approval before using HCC equipment or services from outside UK and Europe. • Requirement to obtain Departmental SIRO approval before using USB storage (which should only be by exception). • Statement that users must not install unauthorised software (only software from approved app stores may be installed by users).
2.1	06/12/21	Kerri Simpson	Updated the social media policy link
3.0	21/10/22	Kerri Simpson	Added Phishing e-mail section and moved to new template
3.1	21/11/2022	Kerri Simpson	Added wording as recommended by the ICO (Information Commissioner s Office) in relation to personal data stored on council devices
3.2	10 November 2023	Kerri Simpson	Added the Artificial Intelligence section.
3.3	2 January 2024	Kerri Simpson	Updated the working from abroad policy changes
3.4	11 January 2024	David Wigley	Replaced “e.g.” with “for example” to align with corporate style guidance. Updated policy statements to include agreed changes: • controls on TikTok use • requirement for users to follow reasonable requests • requirement for user supplied devices to have their software updated and within vendor support

Corporate Acceptable Use Policy

Hampshire County Council

Version	Change date	Changed by	Brief Description
3.5	11 November 2024	Kerri Simpson	Added the link to the Mobile Messaging App Usage Policy
3.5.1	13 March 2025	Nick Manley	Added items in section 3 regarding mouse wigglers and removing network credentials on shared/pool devices
3.5.2	11 April 2025	David Wigley	Added items in Section 3 regarding access to broadcast media and other film and television content. Added an item in Section 4 regarding extremism and terrorism in accordance with our Prevent obligations.
3.5.3	06 August 2025	Clark Williams	Updated link to Social Media Policy
3.6	10 November 2025	Kerri Simpson	Added a paragraph for use of corporate telephony
3.61	29 September 2026	Kerri Simpson	Annual review: updated links and change of role title