Chichester City Council

IT Equipment and Systems Acceptable Use Policy

1. Introduction and general principles

1.1. IT and communications systems are of key importance to the City Council. These systems must be used appropriately. There is a significant risk of damage to the Council and its reputation if you misuse them.

1.2. In this Policy, we set out the standards we require you to follow when using these systems and equipment. We also explain when we will monitor your usage, and for what purpose, and set out the sanctions for breaches of this Policy.

1.3. For Officers, please note that this Policy does not form part of your contract with the City Council.

1.4. The City Council reserves the right to amend or remove this Policy at any point.

1.5. This Policy applies to all Members and Officers of the City Council and anyone who has access to it's IT and communications systems. This may include, but is not limited to, contractors, agency workers, casual workers, interns, volunteers and members of the public who have been co-opted on to any of the City Council's Committees, Sub-Committees or Working Groups.

1.6. The Council will ensure that training is provided for Members and Officers in connection with this policy.

1.7. Agendas and committee papers will be sent electronically. It is not expected that these will be provided in a paper format, unless due to exceptional circumstances, e.g. failure of laptop.

1.8. Use of City Council issued devices must be in accordance with the Data Protection Act 2018 and General Data Protection Regulations (GDPR) and you are expected to familiarise yourself with these principles as set out in the Council's GDPR policy (details in section 10).

1.9. All data and emails stored on City Council issued devices and transacted as part of Council business are the property of Chichester City Council and may be accessed at any time further to the City Council's Data Protection and GDPR policies and General Privacy Statement.

2. City Council issued devices

2.1. The City Council undertakes to supply appropriate devices to Councillors and Officers during their time in office.

2.2. For the avoidance of doubt, City Council issued devices can include, but are not limited to, mobile phones, tablets, laptops, desktop computers, monitors and printers and other peripherals. Further, devices are issued to assist in the specific and limited purpose of carrying out City Council business.

2.3. Any additional peripherals such as printers, additional keyboards or supports that may be desirable are at the expense of the Councillor/Officer. Certain exceptions apply if the provision of such devices is deemed critical to the individual being able to perform their duties.

2.4. The cost of ink and paper used for business specific printing on personal printers may be claimed back through the Council Services and Support Manager. Requirements must be discussed prior to incurring the costs.

2.5. You are responsible for the security of any device issued to you by the City Council. You must not let any of your devices be used by anyone else, whether at work or at home, unless it is as part of authorised support being provided to resolve issues with the device or installed systems.

2.6. When working, either in the office or remotely, you are responsible for the security of the device. The screen should always be locked if it is left unattended, even for short periods of time.

2.7. You must not remove or tamper with any software systems installed on City Council devices. If you have an issue in relation to the device or any software installed on the device, you should contact City Council Officers for advice.

2.8. It is not permitted for you to install any software or systems that are unrelated to City Council business on a Council device. Any such requirement should be discussed with the Town Clerk.

2.9. Device passwords will not normally be distributed as they will be preconfigured. You should use a unique PIN for each electronic device issued to you. This will be set up at the point the device is issued. You should keep all PINs and passwords confidential and should not share them with anyone else (save as outlined below). You should change your passwords/PINs if prompted by the system or asked to do so as part of authorised City Council support. If you forget your PIN you should contact Officers for advice.

2.10. You must provide us with details of all passwords/PINs on request but only in relation to official City Council support.

2.11. No attempt to hack or change the device and/or Microsoft account passwords is permitted. If you are experiencing problems accessing the device or Microsoft account you should contact the City Council offices for advice.

2.12. All City Council system accounts will be deactivated at the end of your Council term for Members and at the end of your employment contract for Officers.

2.13. Every effort to protect both hardware and software from misuse and/or damage must be made. You may be liable for any repair and/or replacement costs if it is deemed that the device or software system has been mistreated or you have been negligent in its care. You must report any loss of, or damage to, City Council issued devices to the Town Clerk immediately.

2.14. If you are issued with portable devices by the City Council, then you must make sure that they are stored safely and securely when being transported. If you are using City Council devices whilst in a public place, you must ensure that others are not able to view your screen. You must make sure that you do not display any confidential information when using City Council devices in public.

2.15. If you are issued with any City Council devices (such as computers, monitors, keyboards or printers) for use then you agree to return it to us on demand and, in any event, at the end of your tenure as a City Councillor or the termination of your employment. You are responsible for maintaining any device issued to you in a good condition. You are responsible for loss of, or damage to, any devices issued to you, other than that caused by reasonable wear and tear.

2.16. The device is covered by the City Council's insurance policy. If the device is lost, stolen or damaged it must be reported to the City Council offices immediately. Insurance cover is limited to the UK and does not cover accidental damage or damage through negligence.

2.17. You are not permitted to take the City Council issued device abroad.

2.18. You are not permitted to contact the City Council's IT provider directly under any circumstances as this incurs a charge to the Council.

3. Systems and data security

3.1. You are always responsible for the protection of City Council data and information sent to the device.

3.2. You must not download or install any software from external sources without the prior approval of the Town Clerk.

3.3. You must not use any Council issued device on public unsecured Wi-Fi unless Officers have installed suitable security measures to protect the security of City Council data.

3.4. City Council laptops and tablets are issued with regularly updated anti-virus software. It is not permitted to tamper with this software or impede its functionality.

3.5. It is not permitted to knowingly introduce viruses or other malicious software on to City Council devices.

3.6. You should review all emails you receive from unknown sources. If you suspect that an email is not genuine, then you should contact the Town Clerk or Council Services and Support Manager as soon as possible. You must not not open the email or any attachments to it.

3.7. You must not reveal confidential data to any third party. This includes, but is not limited to, sensitive data (as defined under the Data Protection Act 2018 and GDPR), computer software course codes, login details and passwords. This may only be done if explicit permission has been given by the Town Clerk in writing and only in accordance with Data Protection Guidelines.

3.8. You must NEVER respond to offers of technical support unless you have previously reported a problem to Officers and have been advised that a support agent will be in touch. If in ANY doubt, you must decline the call and contact the City Council Officers for further advice.

4. Email

4.1. The following rules should be followed when using email:

a You should avoid the use of slang, emojis and 'text speak' when sending business related emails.

b Always consider the relevant recipients when sending an email – do not copy messages unnecessarily widely or use the Reply All function if it is not needed.

c You should not forward chain emails or send jokes.

d It is NOT permitted to forward on Council business emails or Council documentation that is not in the public domain to personal email accounts or other electronic storage media. Further, it is not permitted to transact City Council business electronically outside of the email accounts and devices issued by the Council.

e Do not send emails which are or might be considered abusive, obscene, discriminatory, harassing or otherwise inappropriate in nature. If you receive such an email, then you should inform the Town Clerk immediately. The City Council has a zero-tolerance policy in relation to bullying and harassmen.. Please the City Council's Code of Conduct (Councillors) or the City Council's Staff Handbook (Officers) for more details.

f Email correspondence is disclosable in legal proceedings. All messages should be treated as being potentially disclosable in a court of law.

g It is possible to enter into a legally binding contract via email. If your job role involves the negotiation of terms which could form a contract, then you should ensure that all correspondence is headed "Subject to contract". It is NOT permitted for Councillors to enter in to contracts on behalf of the City Council or suggest the intention to do so. Advice on this should be sought from the Town Clerk.

h You must not use your personal email address for work purposes.

5. Internet

5.1. Internet access in City Council properties is provided primarily for work.

5.2. Personal use of the internet is only permitted on the basis set out in section 6 and on devices connected to the City Council's Guest network.

5.3. The use of the internet to access and / or distribute any kind of offensive material is not permitted. It is forbidden to send, solicit or download inappropriate materials of any type using the City Council issued device. This includes, but is not limited to, pornographic images and materials inciting

and/or promoting violence, drug abuse or illegal activities; through the internet or via email technology.

5.4. The City Council issued device must not be used for online gambling, accessing or transmitting pornography, transmitting copyright information and / or software material, posting confidential information about Councillors, employees or the public or suppliers to the Council, or to make malicious statements to any person.

5.5. You must not use our systems to post on chat rooms or social media sites unless you are doing so as part of your job. For more guidance in this area, please refer to the City Council's Social Media policy.

5.6. Use of social media on any City Council issued device must be in accordance with the Council's Social Media Policy if social media is to be accessed using the device. Further, users are reminded that use of social media on ANY device where comments made or materials uploaded can be deemed to be on behalf of the City Council or connected with your role as a Councillor or Officer; are also governed by the Social Media Policy.

5.7. In some cases, remote monitoring of websites, emails sent and/or other activity may take place, but only in cases where suspicion of illegal or inappropriate behaviour regarding the activity or the use of the City Council device exists. This may only be carried out under the supervision of the Town Clerk. Under most circumstances no information that is discovered will be disclosed to a third party and all investigations will strictly adhere to the Data Protection Act 2018 and GDPR. In more serious cases, investigations may be undertaken in conjunction with the Monitoring Officer and in line with the Regulation of Investigatory Powers (RIPA) Act 2000.

5.8. Any purchases made through websites on the City Council issued device are the liability of the individual Councillor or Officer and shall not be reimbursed by Chichester City Council. Councillors are not permitted to make purchases on behalf of the City Council. Officers may only make purchases in line with their duties and with the explicit consent of the Town Clerk.

6. Personal use of email and the internet

6.1. Limited personal use of the City Council device is permitted. However, any such use MUST comply with these guidelines and MUST NOT compromise the City Council data and/or systems on the device. If in doubt, you should NOT use the device for personal activities.

6.2. Councillors should not use City Council issued devices for casual internet browsing or setting up of personal email accounts.

6.3. The Council provides email and internet access for work-related purposes. Limited personal use is permitted. However, excessive personal use of these resources during working hours may result in disciplinary action under the City Council's Disciplinary Policy as outlined in the current version of the City Council Staff Handbook.

6.4. The following guidance should be followed:

a Personal use of City Council devices should be kept to a minimum.

b Personal use should not interfere with your work commitments

c Personal use must not commit the business to any costs.

d Personal use must always comply with the relevant policies as outlined in the Staff Handbook as well as the relevant Data Protection and GDPR policies.

e Use of personal devices for internet and email use is permitted in Officers' own time subject to the above limitations and only when personal devices are connected to the City Council Guest network.

f It is NOT permitted to connect personal devices to the City Council Private network.

7. Monitoring

7.1. Use of City Council provided IT and communications systems (including computer, internet, email and telephone) may be monitored. Any such monitoring will only be carried out to the extent permitted by law and in accordance with the City Council's Data Protection and GDPR policies.

7.2. The City Council may monitor and check emails and internet usage for reasons including, but not limited to, the following:

a To assess compliance with City Council rules and policies

b To investigate alleged wrongdoing by you or others

c To monitor performance, particularly as part of a performance management process. You will be advised if this is the case.

d To retrieve lost messages

e To access messages and information if you are unable to do so directly (for example due to illness or other absence)

f To comply with the City Council's legal obligations

8. Use of personal devices for work purposes – NOT CURRENTLY IN PLACE EXCEPT FOR DECISIONS SYSTEM – SUBJECT TO CHANGE OF GENERAL POLICY

8.1. It is not permitted to use personal devices for business purposes, other than with specific systems designed not to download Council data to those devices. Any use must be in accordance with the following rules:

a Use of any personal device for business purposes must be approved by the Town Clerk, subject to a policy agreed by the City Council, before it can be connected to any City Council systems and be used for work purposes. Any connection of a personal device to City Council systems may require the installation of additional security measures prior to using the device for work. Any costs incurred would subject to City Council policy, be borne by the Council.

b Any software systems installed by us to allow your device to be used for work must not be tampered with or removed by you.

c The City Council reserves the right to monitor, intercept and remove any content on your device which has been created by us or on our behalf to the extent permitted by law or for our legitimate business purposes. Such activity would be subject to the City Council's Data Protection Policy and Privacy Statementl. Due to the personal ownership of the device, the City Council is aware that inadvertent monitoring, interception, review and removal of personal data may occur. You should have no expectation of privacy in relation to any data on the device if you are using it for work purposes.

d You must delete any data relating to the Council which is stored locally on your Device as soon as it is no longer required.

e You must pay all costs associated with your Device and its use, including technical support, other than those incurred in installing the additional security measures under 8.1(a).

f If a situation arises where there is cause for concern regarding data integrity or City Council system use through your personal device, you must cooperate with the City Council and allow your device to be inspected at any time on request. You would be expected to provide any necessary passwords or login details to enable us to have full access.

g You must report any loss of the device immediately to the Town Clerk to allow for access to City Council systems to be disabled as required to protect system and data integrity.

h In the event of your Councillor tenure ending, your term of employment with the City Council ending or you decide to sell or transfer your personal device, agree to present your device to

City Council Officers prior to transfer/termination to allow for the removal of all Council software and data from it.

8.2. Any breach of these rules may result in permission to use your device for work purposes It may also result in disciplinary action up to and including dismissal or, in the case of a contractor or agency worker, the termination of your engagement. In the event of this happening you would be required to present your device to City Council Officers to allow for the removal of all Council software and data from it.

9. Breaches of this Policy

9.1. Any breaches of this Policy will be handled under the City Council's Code of Conduct (Councillors) or Staff Handbook (Officers). In the case of agency workers, contractors, casual workers and interns, we reserve the right to terminate your engagement in the event of a breach or an alleged breach of this Policy.

9.2. Certain behaviours in breach of this Policy may give rise to a criminal offence or other public concern. We may pass any evidence collated to the police or other relevant authority.

9.3. If you become aware of conduct of others which may be in breach of this Policy, you should report your concern immediately to your line manager or, in the event that the concern is regarding your line manager, to the Town Clerk (Officers) or to the Town Clerk if it concerns Councillors. For Officers, the Whistleblowing Policy in the Staff Handbook provides further guidance.

10. Useful links and contacts

10.1. The following internal policies are referred to in this Policy and contain additional information and guidance [*amend as appropriate*]:

a Staff Handbook - https://chichestercity.gov.uk/wp-content/uploads/2024/11/Staff-Handbook-V1-November-2024-website-links-added-compressed.pdf

b Social Media Policy

c Data Protection Policy and Privacy Statement - https://chichestercity.gov.uk/terms-conditions

10.2. The Town Clerk can be contacted at any time in relation to the matters detailed in this policy via clerk@chichestercity.gov.uk

10.3. Any suspicious emails or IT related contacts should be reported immediatelyIf you receive a suspicious email, please forward it directly to administration@chichestercity.gov.uk for the attention of the Council Services and Support Manager.

11. Administration of the Computers, Email and Internet Policy

11.1. The Town Clerk and Council Services and Support Manager are responsible for the administration of the City Council's devices, Email and Internet Policies. Should you have any feedback, please contact them direct.

Date policy adopted: 17 December 2025

Minute reference: COUNCIL2025/26

AGREEMENT TO THE PRINCIPLES OF THE CITY COUNCIL IT EQUIPMENT AND SYSTEMS ACCEPTABLE USE POLICY

I, ... , a Member/Officer of Chichester City Council, agree to the principles laid out in the City Council's IT and Acceptable Use Policy.

I understand that I may be financially responsible for any damage to or loss of the device due to accidental damage or negligence.

I understand that the device I have been provided with is the property of the City Council.

I agree to the principles of use of the device as set out above and agree to receive all Committee papers and associated Council correspondence electronically via my City Council account on the device.

I agree to return the device immediately upon the completion of my tenure as a City Councillor or the end of my employment with the City Council.

Device serial and asset numbers: ……..

Signed: ……..

Print name: ……..

Date: ……..