Last Reviewed Dec 2021
Next Review Date 2025

Computer, Email & Internet Policy

1. Computer

1.1 Some employees have access to computers at work for use in connection with the Council's business. Computers are provided to employees to undertake business-related activities only. Employees who are discovered unreasonably using the Council's computers for personal and private purposes will be dealt with under the Council's disciplinary procedure.

1.2 Vandalism of, or otherwise intentionally interfering with, the Council's computers/network constitutes a gross misconduct offence and could render the employee liable to summary dismissal.

2. Security

As many computer files contain some form of confidential or otherwise sensitive business information, the Council takes the security of these files very seriously. With this in mind, there are some basic security precautions that all employees must abide by as follows:

a) if an employee needs to leave their computer for a long period of time, log off - never leave an unattended computer logged on
b) computer passwords are considered Diss Town Council's confidential information even if the employee is using their personal password for social networking to login to our work systems. When creating a computer password, do not use one that is obvious, such as your date of birth or the name of a close family member
c) Employee's should always keep their password private, do not write it down and do not divulge it to anyone else (including other members of staff), except for Town Clerk/Deputy Town Clerk
d) always shut down the computer when you go home at the end of the day
e) if an employee notices any suspicious activity, for example an employee trying to gain unauthorised access to another member of staff's computer, notify your line manager immediately
f) if an employee is provided with a Town Council computer for use in their home, family members are not allowed to use it.

3. Data

3.1 The computers and the data they contain are provided to undertake business-related activities and to enable employees to carry out their job duties. As such, data should not be amended, deleted, copied or taken away unless this is both specifically related to the work employees are undertaking and employees have the authority to make such amendment, deletion or copy. In particular, employees should not delete or amend any documentation or programs which are stored on the Council's communal drives without the requisite level of authority to do so.

3.2 Non work-related data should not be copied onto or stored on Council computers.

4. Use of portable storage devices

Some employees may be provided with portable storage devices, such as memory sticks and portable hard drives, which can be plugged into the USB port of a computer. Whilst they are provided to allow for the copying and transferring of files and images between an employee's desktop or laptop computer, their small size and storage capacity makes them vulnerable to misuse. For this reason, any employee issued with these devices must

not transfer any data to a third-party computer (including one at home) without first having obtained approval from their manager. From time to time, user guidelines will be produced on the usage of such devices and employees will be expected to follow them. Any employee who transfers files to a third party without permission is likely to be subject to disciplinary action (see also policy 8). If this involves the deliberate transfer of sensitive commercial information to a competitor, it will be treated as gross misconduct.

5. Software

Software that the employee needs to use to carry out their job duties will be provided and installed on the Council's computer for the employee. Installation of any non-approved software is prohibited. This includes screen savers and wallpapers. Only the IT department has the authority to load new software onto the network system. Even then, software may be loaded only after having been checked for viruses.

6. Viruses

6.1. The Council's computer network makes it vulnerable to viruses & all computers have virus protection software installed. Re-configuring or disabling this software is prohibited.

6.2. If an employee's computer starts to behave strangely or the employee suspects it may have become infected with a virus, turn it off immediately and contact the IT department.

7. Remote access

7.1. Some employees may spend at least part of their working week on Council business away from the premises. These employees and any others who may work remotely on an informal basis should be aware that all aspects of this policy apply equally to them. Remote working employees will also be expected to comply with any additional guidelines that may be introduced in order to reduce the likelihood of the Council's computer networks being compromised as a result of remote access.

7.2. Employees must not allow any family members or other third parties to either use the Council's computer equipment (including software) or to access or view its internal IT networks.

8. Managers' duties

8.1. Managers will be required to notify the IT department in advance of any computer users that will be leaving the Council. This should be done at least two weeks before the employee leaves, so that the individual's account can be closed down on their departure.

8.2. Likewise, managers should notify the IT department in advance of any new computer users that will be starting work for the Council. This should be done at least two weeks before the employee starts, so that the individual's account can be set up ready for their start date.

8.3. From time to time, the Council will review its storage of confidential information and the media upon which it is stored. Managers will be expected to co-operate in terms of identifying such files, the employees or other staff with access to them and the file locations.

9. E-Mail & Internet

9.1. Some employees have access to e-mail and the Internet for exclusive use in connection with the Council's business and as part of the normal execution of their

job duties. The purpose of these rules is to protect the Council's legal interests. Unregulated access increases the risk of employees inadvertently forming contracts through e-mail and increases the opportunity for wrongful disclosure of confidential information.

9.2. As such, all e-mails sent internally and externally, e.g. to clients and customers, must follow the Council's designated style, which will be supplied to authorised users. Furthermore, employees must not, under any circumstances, include unacceptable, offensive, derogatory or profane language within the text of any internal or external e-mail. Failure to follow house style and the rules on use of language is a disciplinary matter and will be dealt with under the Council's disciplinary procedure. E-mail should not be used for unsolicited correspondence or marketing campaigns and employees may not commit the Council financially by e-mail unless they have been granted a specific level of delegated authority to do so.

9.3. Employees who are authorised users are not permitted to surf the Internet or to spend excessive time "chatting" by e-mail for personal and private purposes during their normal working hours. Employees are also prohibited from using e-mail to circulate any non-business material. Not only does excessive time spent online lead to loss of productivity and constitute an unauthorised use of the Council's time, sexist, racist or other offensive remarks, pictures or jokes sent by e-mail are capable of amounting to unlawful harassment. As "cyber bullying" is an emerging risk, employees are also prohibited from using the Council's electronic communications as a means of intimidating or bullying employees or third parties.

9.4. Employees who are discovered contravening these rules may face serious disciplinary action under the Council's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal. Use of instant messaging systems must be expressly approved in advance by the employee's manager.

9.5. Employees who are authorised users are permitted to surf the Internet for personal purposes outside their normal working hours. The Council considers acceptable personal use of the Internet to include activities such as personal online shopping, booking holidays and banking. It does not include visiting online gambling sites or participating in online gaming. Employees should note that any purchases or other transactions made online whilst at work are made entirely at their own risk.

9.6. Employees must never use their work e-mail address to make orders for personal goods and services or to sell their personal goods and services or to sign up for any services (except those expressly authorised by the Council). Likewise, if an employee wishes to make a complaint to the third-party supplier or manufacturer about personal goods or services received, a work e-mail address must never be used under any circumstances. These are entirely personal transactions and so the employee must not hold themselves out as acting for or on behalf of the Council or must not in any way indicate that the transaction is connected to the Council.

9.7. Logging on to sexually explicit websites or the downloading and/or circulation of pornography or other grossly offensive, illegal or obscene material or using the Internet for gambling or illegal activities constitutes gross misconduct and could render the employee liable to summary dismissal under the Council's disciplinary procedure. "Rogue" websites exist that appear harmless but instead direct the user automatically to another website that may contain inappropriate material. If this occurs, please contact the IT department immediately.

10. E-Mail & Internet

10.1. When logging on to and using social networking and video sharing websites and blogs ("social media") at any time, including personal use on non-Council computers outside the workplace and outside normal working hours, employees must not:

a) use social media in a way that breaches any of the Council's other policies - if an Internet post would breach any of these policies in another forum, it will also breach them in an online forum

b) other than in relation to the Council's own social media activities or other than where expressly permitted by the Council on business networking websites such as LinkedIn, publicly identify themselves as working for the Council, make reference to the Council or provide information from which others can ascertain the name of the Council (and in any event they should not hold themselves out as associated with the Council on any social media website after termination of employment)

c) other than in relation to the Council's own social media activities or other than where expressly permitted by the Council on business networking websites such as LinkedIn, write about their work for the Council - and, in postings that could be linked to the Council, they must also ensure that any personal views and opinions expressed are clearly stated to be theirs alone and do not represent those of the Council

d) create a social media account that could be mistaken for a Council social media account

e) create a social media account or profile that impersonates one or more of the Council's employees, clients, customers, contractors or suppliers

f) use the Council's logos, trademarks or other corporate artwork on a personal social media account or conduct themselves in a way that is potentially detrimental to the Council or directly or indirectly brings the Council or its clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content or sharing inappropriate content posted by others

g) allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Council, for example by criticising or arguing with such persons or using abusive or threatening language towards them

h) include personal information or data about the Council's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Council reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 1998 which is a criminal offence

i) make any derogatory, offensive, discriminatory, disrespectful, untrue, negative, misleading, critical, disparaging or defamatory comments or statements about the Council, its employees, clients, customers, contractors or suppliers (an employee may still be liable even if the Council, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Council reasonably believes they are identifiable)

j) air grievances about the Council or any of its activities

k) make any comments about the Council's employees that could constitute unlawful discrimination, harassment, victimisation or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory, or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation

l) disclose any confidential, proprietary or sensitive information belonging to the Council

m) breach copyright or any other proprietary interest belonging to the Council, for example, using someone else's images or written content without permission or failing to give acknowledgement where permission has been given to reproduce particular work - if employees wish to post images, photographs, personal details or videos of their work colleagues or clients, customers, contractors or suppliers on their online profile, they should first obtain the other party's express permission to do so.

10.2. Employees should remember that social networking websites are a public forum, even if they have set their account settings at a restricted access or "friends only" level, and therefore they should not assume that their entries on any website will remain private. Employees must also be security conscious when using social networking websites and should take appropriate steps to protect themselves from identity theft, for example by restricting the amount of personal information they give out, such as date and place of birth, schools attended, family names and favourite football team. This information may form the basis of security questions and/or passwords on other websites, such as online banking.

10.3. Employees who are discovered contravening these rules, whether inside or outside the workplace, may face serious disciplinary action under the Council's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal.

11. Downloading information from the Internet and file sharing

11.1. Due to our faster computer networks, employees may be tempted to make illegal downloads of material that is subject to copyright. This includes, but is not limited to, music, film and business software. As this and any subsequent file sharing of this material constitutes an infringement of copyright, it is prohibited on any Council computer. This also applies to any download or dissemination of material made outside of normal working hours. Any breach is likely to lead to disciplinary action being taken.

11.2. The employee may need to download documents and information from the Internet in order to undertake their job duties. The employee should only download documents and information that they are sure about and which is required to fulfil the job duties which are being undertaken. With the rapid spread of computer viruses via the Internet, care should be taken when accessing websites that the employee is not familiar with or when downloading documents or information.

11.3. The employee must not download any programs from the Internet without the prior approval of the IT department. Some websites require additional add-in software to display the page completely. These add-ins usually provide additional sound or visual effects. Under no circumstances should these be downloaded without the prior approval of the IT department.

12. E-mail and Internet monitoring

12.1. The Council reserves the right to monitor employees' internal and external e-mails and use of the Internet, both during routine audits of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

12.2. The purposes for such monitoring are to:

a) promote productivity and efficiency

b) ensure the security of the system and its effective operation

c) ensure there is no unauthorised use of the Council's time, e.g. that an employee has not been using e-mail to send or receive an excessive number of personal communications

d) ensure the smooth running of the business if the employee is absent for any reason and communications need to be checked

e) ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment

f) ensure that inappropriate websites are not being accessed by employees.

12.3. When monitoring e-mails, the Council will, except in exceptional circumstances, confine itself to looking at the address and heading of the e-mails. However, where circumstances warrant it, the Council may open e-mails and access the content. In this case, the Council will avoid, if possible, opening e-mails clearly marked as private or personal.

12.4. The Council reserves the right to restrict, deny or remove e-mail or Internet access to or from any employee.

13. E-mail guidelines

In addition to following the Council's designated house style in all internal and external e-mail and the provisions on reading and storing e-mails, the Council recommends that employees follow these e-mail guidelines:

a) use the subject line to specify exactly what the e-mail is about

b) only mark an outgoing e-mail as "urgent" or "high priority" if that is really the case; not because a swift reply is expected or desired from the recipient

c) be concise in the body of your text

d) if an outgoing e-mail is not urgent, always give the recipient adequate time to reply

e) if an issue or query in an e-mail is urgent, consider telephoning the intended recipient first and then following up with a confirmatory e-mail later

f) answer all incoming e-mails within 24 hours (if only to acknowledge receipt)

g) if the employee cannot give a response at that point, state when you will be able to reply in full and/or what you are doing to find out the answer or resolve the issue.

14. E-mail viruses and spam

14.1. All incoming and outgoing external e-mails are checked for computer viruses and, if a virus is found, the message will be blocked. E-mails may also be checked for other criteria, for example, having an attached image file or containing offensive or inappropriate material or including a “banned” word or from a “banned” user under the criteria in the Council’s spam software which indicates the message is spam. Again, the e-mail will be blocked. The Council reserves the right for the IT department to block and then read these messages to ascertain whether they are business-related.

14.2. If an employee receives an e-mail or data file that is in a format or comes from a source that they do not recognise, do not open the item but contact the IT department immediately. Any executable (.exe) files received by e-mail must be referred to the IT department for clearance before any other action is taken.

14.3. If an employee receives any unsolicited e-mails or spam that manages to bypass the Council’s spam software, the employee must not respond in any way. Please forward the e-mail to the IT department and they will add the sender to the list of banned users. Some spam e-mails may offer the option to opt out of receiving them. Be aware that this is sometimes used as a way by unscrupulous spammers of validating a live e-mail address.

15. Social media

Social media is an interactive online media that allows users to communicate instantly with each other or to share data in a public forum. It includes social and business networking websites such as Facebook, Reddit, Twitter and LinkedIn. Social media also covers video and image sharing and blogging websites such as YouTube, Instagram, Google+, Tumblr and Flickr, as well as personal blogs, any posts made on other people’s blogs and all online forums and noticeboards. This is a constantly changing area with new websites being launched on a regular basis and therefore this list is not exhaustive. This policy applies in relation to any social media that employees may use.

16. Use of social media at work

16.1. Employees are only permitted to log on to social media websites or to keep a blog using the Council’s IT systems and equipment outside their normal working hours (for example, during lunch breaks or after the working day has finished) and this must not under any circumstances interfere with their job duties or have a detrimental effect on their productivity. This includes laptop and hand-held computers, or devices distributed by the Council for work purposes. The Council nevertheless reserves the right to restrict access to this type of websites at any time. Where employees have their own computers or devices, such as laptops and hand-held personal devices

such as smartphones, again they must limit their use of social media on this equipment to outside their normal working hours.

16.2. However, employees may be asked to contribute to the Council's own social media activities during normal working hours, for example by writing Council blogs or newsfeeds, managing a Facebook account or running an official Twitter or LinkedIn account for the Council. Employees must be aware at all times that, while contributing to the Council's social media activities, they are representing the Council and they must not post any personal content on any Council social media account that they are authorised to use.

17. Council's social media activities

17.1. Where employees are authorised to contribute to the Council's own social media activities as part of their work, for example for marketing, promotional and recruitment purposes, they must adhere to the following rules:

a) use the same safeguards as they would with any other type of communication about the Council that is in the public domain
b) ensure that any communication has a purpose and a benefit for the Council
c) obtain permission from their Line Manager before embarking on a public campaign using social media
d) request their Line Manager to check and approve content before it is published online
e) not under any circumstances post any personal content or express any personal opinions that do not represent those of the Council
f) follow any additional guidelines given by the Council from time to time.

17.2. In addition, such social media accounts which are operated for business purposes (and their contents) belong to the Council and therefore these accounts used by an employee during employment may not be used after termination of employment. The Council may also ask the employee to supply their usernames and passwords either on termination of employment or at any other time and in either case the employee must supply them on request.

18. Social media rules

18.1. The Council recognises that many employees make use of social media in a personal capacity outside the workplace and outside normal working hours. While they are not acting on behalf of the Council in these circumstances, employees must be aware that they can still cause damage to the Council if they are recognised online as being one of its employees. Therefore, it is important that the Council has strict social media rules in place to protect its position.

18.2. When logging on to and using social media websites and blogs at any time, including personal use on non-Council computers outside the workplace and outside normal working hours, employees must not:

a) use social media in a way that breaches any of the Council's other policies - if an Internet post would breach any of these policies in another forum, it will also breach

them in an online forum

b) other than in relation to the Council's own social media activities or other than where expressly permitted by the Council on business networking websites such as LinkedIn, publicly identify themselves as working for the Council, make reference to the Council or provide information from which others can ascertain the name of the Council (and in any event they should not hold themselves out as associated with the Council on any social media website after termination of employment)
c) other than in relation to the Council's own social media activities or other than where expressly permitted by the Council on business networking websites such as LinkedIn, write about their work for the Council - and, in postings that could be linked to the Council, they must also ensure that any personal views and opinions expressed are clearly stated to be theirs alone and do not represent those of the Council
d) create a social media account that could be mistaken for a Council social media account
e) create a social media account or profile that impersonates one or more of the Council's employees, clients, customers, contractors or suppliers
f) use the Council's logos, trademarks or other corporate artwork on a personal social media account
g) conduct themselves in a way that is potentially detrimental to the Council or directly or indirectly brings the Council or its clients, customers, contractors or suppliers into disrepute, for example by posting images or video clips that are inappropriate or links to inappropriate website content or sharing inappropriate content posted by others
h) other than in relation to the Council's own social media activities or other than where expressly permitted by the Council on business networking websites such as LinkedIn, use their work e-mail address when registering on such sites or provide any link to the Council's website
i) allow their interaction on these websites or blogs to damage working relationships with or between employees and clients, customers, contractors or suppliers of the Council, for example by criticising or arguing with such persons or using abusive or threatening language towards them
j) include personal information or data about the Council's employees, clients, customers, contractors or suppliers without their express consent (an employee may still be liable even if employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Council reasonably believes they are identifiable) - this could constitute a breach of the Data Protection Act 2018 which is a criminal offence
k) make any derogatory, offensive, discriminatory, disrespectful, untrue, negative, misleading, critical, disparaging or defamatory comments or statements about the Council, its employees, clients, customers, contractors or suppliers (an employee may still be liable even if the Council, its employees, clients, customers, contractors or suppliers are not expressly named in the websites or blogs as long as the Council reasonably believes they are identifiable)
l) air grievances about the Council or any of its activities
m) make any comments about the Council's employees that could constitute unlawful discrimination, harassment, victimisation or cyber-bullying contrary to the Equality Act 2010 or post any images or video clips that are discriminatory, or which may constitute unlawful harassment or cyber-bullying - employees can be personally liable for their actions under the legislation
n) provide references for other individuals on social media websites, as such references could be attributed to the Council and create legal liability for both the author of the reference and the Council
o) disclose any proprietary or sensitive information belonging to the Council, for example information about the Council's work, its products and services, technical developments, future business plans, staff morale and anything else that is not already in the public domain

18.3. Employees must remove any offending social media content immediately if they are asked to do so by the Council.

18.4. On termination of employment or once notice to terminate employment has been given, employees must, on request, disclose to the Council a full list of all work and business contacts that they hold on all devices or on all social and business networking accounts. The Council may then require the departing employee to delete any or all such work and business connections from their devices (including from personal devices). The Council may also require written confirmation from the employee that these provisions have been complied with.

18.5. Employees must also surrender all login and password details for accounts run on the Council's behalf or where an account has been used to promote and/or market the Council's business activities on the termination of employment or whenever so requested by the Council.

18.6. Employees should remember that social media websites are public fora, even if they have set their account privacy settings at a restricted access or “friends only” level, and therefore they should not assume that their postings on any website will remain private.

18.7. Employees must also be security conscious when using social media websites and should take appropriate steps to protect themselves from identity theft, for example by placing their privacy settings at a high level and restricting the amount of personal information they give out, e.g. date and place of birth. This type of information may form the basis of security questions and/or passwords on other websites, such as online banking.

18.8. Should employees notice any inaccurate information about the Council online or which breaches this policy or otherwise brings the Council into disrepute, they should report this to their Line Manager in the first instance.

19. Social media monitoring

19.1. The Council reserves the right to monitor employees’ use of social media on the Internet, both during routine audits or random spot checks of the computer system and in specific cases where a problem relating to excessive or unauthorised use is suspected.

19.2. The Council will only monitor use of social media on the Internet where we have a lawful basis for doing so. The business purposes for such monitoring are to:

a) establish the existence of facts
b) ascertain compliance with regulatory or self-regulatory requirements, practices or procedures
c) assess standards of employee performance and conduct and promote productivity and efficiency
d) investigate or detect any unauthorised use of the systems
e) ensure the security of the systems and networks and their effective operation
f) ensure the smooth running of the business by checking whether there are any relevant business communications that need to be dealt with

g) ensure that the Council's rules, policies and procedures are being complied with
h) record transactions
i) promote customer satisfaction
j) ensure that the systems are not being used for any unlawful purpose or activities that may damage the Council's reputation
k) make sure there is no unauthorised use of the Council's time
l) perform effective internal administration
m) ensure that inappropriate, restricted or blocked websites are not being accessed and that offensive or illegal material is not being viewed, sent, downloaded or circulated
n) ensure that all employees are treated with respect and dignity at work, by discovering and eliminating any material that is capable of amounting to unlawful harassment
o) protect the privacy of personal data, trade secrets and sensitive or confidential Council information and ensure there is no breach of confidentiality or data protection provisions.

19.3. Members of the IT department are authorised to monitor social media on the Internet during routine audits or random spot checks and they may also be instructed to do so by managers where a problem is suspected. Access to the results of monitoring is restricted to the IT department and to those managers who are authorised to access them in accordance with the purposes outlined above. Disclosure of the results of monitoring to other third parties will only be made in accordance with the purposes outlined above and will be limited to:

a) the police and other law enforcement agencies, where the results could assist in the prevention or detection of a crime or the identification and prosecution of an offender
b) prosecution agencies, such as the Crown Prosecution Service
c) relevant legal representatives
d) managers involved with Council disciplinary and performance management processes

19.4. The Town Clerk or Council Leader (or another senior officer acting in their absence) is the only person who is permitted to authorise disclosure of information to external third parties such as law enforcement agencies.

19.5. Social media monitoring may involve obtaining an itemised log of all social media websites and individual web pages visited, as well as the date and time of access. Where the particular circumstances warrant it, it may also involve accessing the actual content posted or circulated on social media web pages.

19.6. The Council is committed to being transparent about how and why employees are monitored and will always consider whether the monitoring measures are proportionate.

19.7. The Council reserves the right to restrict, deny or remove Internet access, or access to particular social media websites, to or from any employee.

20. Contravention of this policy

20.1. Failure to comply with any of the requirements of this policy, including failing to remove any social media content that in itself breaches this policy, is a disciplinary offence and may result in disciplinary action being taken under the Council's disciplinary procedure. Depending on the seriousness of the offence, it may amount to gross misconduct and could result in the employee's summary dismissal. Any employee suspected of committing a breach of this policy will be required to co-operate with the investigation, which may involve handing over relevant login and password details.

20.2. In addition, employees could face legal proceedings if comments they post about the Council or named individuals are found to have harmed their reputation.