Nelson Town Council
Town Hall
Market Street
Nelson
Lancashire BB9 7LG

Tel: 01282 697079
Email: info@nelsontowncouncil.gov.uk
Website: www.nelsontowncouncil.gov.uk

Social Media, Internet and Email Policy

The terms 'Council' and 'employer' referred to herein refers to Nelson Town Council and applies to all areas of its controlled functions and responsibilities.

Who is covered by the policy?

This policy applies to all Nelson Town Council Staff including all of its employees, officers, contractors, home-workers, part-time and fixed-term employees, secondees, temporary Staff, casual Staff, agency Staff and volunteers ('Staff').

This policy does not form part of your terms and conditions of employment and Nelson Town Council reserves the right to amend the policy at any time.

All Staff are required to read and sign the policy by 1st May 2019 after which time it shall take effect in any event.

Purpose of policy

Nelson Town Council must ensure the requirements of the General Data Protection Regulations 2018 and other Data Protection Laws are met.

This policy supplements our Internet and Email Policy and Use of Social Networking Sites Policy contained within the employee handbook.

This policy is intended to help Staff of Nelson Town Council make appropriate decisions about the use of internet, email and social media such as Twitter, Facebook, Google+, LinkedIn, Wikipedia, Whisper, Instagram, Tumblr and all other social networking sites to include (but not limited to) the internet, video, picture and audio postings and blogging.

This policy applies to use of social media, email and internet for Council business purposes as well as personal use that affects the Council in any way.

This policy outlines the standards Nelson Town Council requires Staff to observe when using the internet, email and social media, the circumstances in which Nelson Town Council will monitor your use of these media and the action that will be taken in respect of breaches of this policy. The principles of this policy apply to use of these media regardless of the method used to access it and covers static and mobile IT/computer equipment, as well as work and/or personal smartphones etc.

Generally

Voicemail, text messages, email, and internet usage assigned to an employee's computer or telephone extensions are solely for the purpose of conducting Council business. Some job responsibilities at the Council require access to the internet and the use of software in addition to the Microsoft Office suite of products.

Only Staff appropriately authorised, for Council purposes, may use the internet to access and download additional software.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for change to minimise risks lies with the Council, with support of the Personnel Committee who will review this policy from time to time to ensure that it meets legal requirements and reflects best practice.

Line Managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all Staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All Staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media, email or the internet should be reported to your line manager and questions regarding the content or application of this policy should be directed to your line manager, the Council Chairman or the Personnel Committee.

This policy shall take effect and be applied immediately regardless of when any instances of abuse or misuse took place; i.e. any instances of misuse or abuse of the policy having taken place before this policy was implemented will still fall for consideration under this policy as and when any complaints or issues are brought to the attention of your line manager, the Council Chairman or the Personnel Committee.

Software needs

Software needed in addition to the Microsoft Office suite of products must be authorised by your line manager before downloading. If you need access to software or websites not currently on the Council network, talk with your manager before downloading.

All reasonable requests that are not considered a network risk will be considered for you and other employees. The purpose of this policy is not to restrict employee access to products that will make you more productive. The goal is to minimize the risk to the Council's network.

Council Owned Equipment

Any device or computer including, but not limited to, desk phones, mobile and smartphones, tablets, laptops, desktop computers, and iPads that the Council provides for your use, should be used only for Council business. Keep in mind that the Council owns the devices **and** the information and or date in any format on these devices. You may not remove or copy any information or date held on any Council device as above. If you leave the Council for any reason, the Council will require that you return the equipment on your last day of work. Failure to return such items on the termination of your employment, will lead to a deduction made from your final pay.

You may use personal electronic devices that are not connected to the Council network to access any appropriate internet site during breaks and lunch breaks only.

Internet Usage

Internet use on Council time or using Council-owned devices that are connected to the Council network is authorised to conduct Council business only. Internet use brings the possibility of breaches of the security of confidential Council information.

Internet use also creates the possibility of contamination to our system via viruses or spyware. Spyware allows unauthorised people outside of the Council potential access to Council passwords and other confidential information.

Removing such programs from the Council network requires IT Staff to invest time and attention that is better devoted to making technological progress. For this reason and to assure the use of work time appropriately for work, we ask Staff members to limit internet use.

Additionally, under no circumstances may Council-owned computers or other electronic equipment, including devices owned by the employee, be used on Council time at work to obtain, view, or reach any pornographic, or otherwise immoral, unethical, or non-council business-related internet sites. Doing so can lead to disciplinary action up to and including termination of employment.

In summary, there should be limited personal use of the internet and of email at work, provided it does not interfere with or impede your normal duties. Such use should take place substantially outside of normal working hours, for example, breaks, lunchtime.

You should not engage in any activity which is illegal, offensive or likely to have negative repercussions for the Council.

Social Media

Some Staff and employees have social media responsibilities in their job description, including event marketing, Council news publishing and recruitment.

Only the Town Clerk/RFO, Assistant Town Clerk, Catering Co-Ordinator and the Council Chairman are permitted to post material on the Council's social media, website and twitter in the Council's name and on our behalf.

We strongly encourage you to limit the use of social media to work-related content during work hours.

Additionally, you are prohibited from sharing any confidential or protected information that belongs to or is about the Council. You are strongly encouraged not to share disparaging information that places your Council or co-workers in an unfavourable light.

Before using Council-related social media you must:

- have read and understood this policy, and;
- have sought approval to do so from your line manager or the Council Chairman.

The Council's reputation and brand should be protected by all Staff. The lives and actions of your co-workers should never be shared online. Please note the preferences of fellow employees who are parents before you use the name of their children online.

In social media participation from work devices or during working hours, social media content that discriminates against any protected classification including age, disability, gender reassignment, marriage and civil partnership, pregnancy or maternity, race, colour, religion or belief, sex, sexual orientation, or genetic information is prohibited.

It is the Council's policy to also recognise weight as qualifying for discrimination protection. Any employee who participates in social media who violates this policy will be dealt with according to the Council disciplinary policy.

You are also personally responsible for what you communicate on social media sites outside the workplace, for example at home, in your own time, using your own equipment. You must always be mindful of your contributions and what you disclose about the Council.

General rules for social media use – including personal use

Whenever you are permitted to use social media in accordance with this policy, you must adhere to the following general rules. The same rules would also apply when using social media outside of work, i.e. for personal or non-Council use:

- Do not post or forward a link to any abusive, discriminatory, harassing, derogatory, defamatory or inappropriate content. This includes potentially offensive or derogatory or defamatory or inappropriate remarks about any other individual.
- A member of Staff who feels that they have been harassed or bullied, or are offended by material posted by a colleague onto a social media website should inform their line manager
- Never disclose commercially sensitive, anti-competitive, private or confidential information. If you are unsure whether the information you wish to share falls within one of these categories, you should discuss this with your line manager.
- Do not post material in breach of copyright or other intellectual property rights.
- Be honest and open, but be mindful of the impact your contribution might make to people's perceptions of the Council.
- You are personally responsible for content you publish – be aware that it will be public for many years.
- When using social media for personal use, use a disclaimer, for example: 'The views expressed are my own and don't reflect the views of my employer'. Be aware though that even if you make it clear that your views on such topics do not represent those of the organisation, your comments could still damage our reputation and action will be taken.
- You should avoid social media communications that might be misconstrued in a way that could damage the Council's reputation, even indirectly.
- Do not post anything that your colleagues or our customers, clients, business partners, suppliers or vendors would find offensive, insulting, obscene and/or discriminatory.
- Do use privacy settings where appropriate but bear in mind that even comments in a restricted forum may be passed on.
- If you have disclosed your affiliation as an employee of the Council you must ensure that your profile and any content you post are consistent with the professional image you present to residents and colleagues.
- You must not request / accept request from clients/service providers of the Council or comment / reply to comments made by clients/service providers on your personal social media accounts.

If you are concerned or uncertain about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your line manager or the Council Chairman.

Any post relating to Council business must be approved by the Council Chairman before posting.

If you see social media content that disparages or reflects poorly on us, you should contact your line manager or the Council Chairman or the Personnel Committee.

Email Usage at the Council

Email is to be used for Council business only. Council confidential information must not be shared outside of the Council, without authorisation, at any time. You are also not to conduct personal business using any Council computer or email.

Please keep this in mind, also, as you consider forwarding non-Council business emails to associates, family or friends. Non-Council business related emails waste Council time and attention.

Viewing pornography, or sending pornographic jokes or stories via email, is considered sexual harassment and will be addressed according to our sexual harassment policy.

The following activities are expressly prohibited:

- The introduction of network monitoring or password detecting software on any Nelson Town Council user machine or part of the network;
- Seeking to gain access to restricted areas of the network;
- The introduction of any form of computer virus;
- Other hacking activities;
- Knowingly seeking to access data which you know, or ought to know, to be confidential and therefore would constitute unauthorised access.

Keep in mind that the Council owns any and all communication sent and received via email or other method or that which is stored on Council computers, mobiles or other equipment. The Council Chairman, Members of the Personnel Committee, management and other authorised Staff have the right to access any material in your email, Council mobile or on your computer at any time. Please do not consider your electronic communication, storage, or access to be private if it is created or stored on any Council system.

If you need additional information about the meaning of any of this communication, please reach out to your line manager, the Council Chairman or the Personnel Committee for clarification.

Monitoring use of social media, email and the internet

Staff should be aware that emails and any use of the internet and social media websites (whether or not accessed for work purposes) may be monitored by your line manager, the Council Chairman or the Personnel Committee or appointed member thereof. Where breaches of this policy are found, action may be taken under the Council's disciplinary procedure.

The Council reserves the right to restrict or prevent access to certain internet sites including social media websites if personal use is considered to be excessive. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for Council-business purposes.

Misuse of social media and other websites can, in certain circumstances, constitute a criminal offence or otherwise give rise to legal liability against you and the Council.

If you notice any use of social media by other members of Staff in breach of this policy please report it to your line manager, the Council Chairman or the Personnel Committee.

Monitoring your usage will mean processing your personal data. You may read more about the data we hold on you, why we hold it and the lawful basis that applies in the employee privacy notice.

Breaches of this policy

Where it is believed that a member of Staff has failed to comply with this policy, they will be subject to the Council's disciplinary procedure. If after being subject to the Council's disciplinary procedure the Staff member is found to have breached this policy, they will face a disciplinary penalty ranging from a verbal warning to dismissal.

The penalty applied will depend on factors such as the seriousness of the breach; the nature of the posting; the impact it has had on the Council or the individual concerned; whether the comments cause problems given the member of Staff's role; whether the Council can be identified by the postings; or other mitigating factors such as the Staff's disciplinary record etc.

Any member of Staff suspected of committing a breach of this policy will be required to co-operate with the Council's investigation, which may involve handing over relevant passwords and login details.

You may be required to remove any social media content that the Council considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

I hereby confirm that I have read and understood this Social Media, Internet and Email Policy and I shall abide by it.

Signed

Print Name

Date