Hyndburn Borough Council

Communications Policy

Contents

1. Introduction

1.1 This policy statement deals with the manner in which Council communications equipment may be used, the use of employee's own communications equipment at work, the circumstances which constitute misuse and how the Council monitor the policy and deal with suspected or actual misuse or misconduct connected with misuse.

1.2 **Employees are advised:**

a) to ensure that you have read and understand the provisions of this policy;
b) to remember the Council's values and reflect these in your communications;
b) that if you have any doubt about whether an action you intend to take using Council communications equipment is permitted by this policy, you should seek advice from a manager or the Head of Audit and Investigations, as appropriate, before you undertake the action;
c) that if you believe that it is necessary, to do your job, to be able to do something which is prohibited by this policy, you should seek advice from your line manager, the Head of ICT, or the Head of Audit and Investigations as appropriate, before you undertake the action.

1.3 This policy statement sets out what is acceptable and unacceptable use of the Council's electronic communications equipment.

1.4 The Council provides employees with a range of electronic communications equipment to enable them to undertake the business of the Council. This equipment is provided primarily for the business purposes of the Council. In this policy, communications equipment means:

(a) fixed point telephones;
(b) PCs (fixed and lap-top – e mail, internet, instant messaging systems and installed software);
(c) fax machines;
(d) mobile phones and smartphones;
(e) iPads and other tablet computers; and
(f) other equipment of a similar nature, as technology is moving rapidly.

1.5 This policy applies both to business and personal use of the Council's equipment with the aim of ensuring that:

- All employees are clear about how and when they may use communications equipment at work and what constitutes misuse;

- Personal use of communications equipment is incidental to work use;
- Personal use of communications equipment in work time is kept to a minimum;
- Communications equipment is not used to cause offence or disturbance to others;
- Employees use communications equipment lawfully and do not expose themselves or the Council to potential liability, either civil or criminal;
- Employees comply with the Data Protection Act and General Data Protection Regulations, including reporting potential breaches without delay to the Data Protection Officer;
- Employees' behaviour does not risk bringing the Council or its officers into disrepute; and
- Employees' behaviour does not compromise Council systems or their security

1.6 **Employees must not assume that their communications, made using Council equipment, whether business related or personal, are private**. While the Council does not seek to make unreasonable intrusions into employees' communications, the Council reserves the right to monitor communications to ensure that Council systems are being used lawfully and appropriately and that this policy is being complied with.

1.7 Employees must have regard to the special risks associated with the speed and ease with which emails can be composed and sent.

(a) Employees must be aware that an electronic communication, even after it has been deleted, may leave a permanent record of the correspondence between sender and recipient which may be used in the future as evidence of misconduct and/or the Council's or the individual's liability for their action.

(b) Employees should also be aware that it is impossible to ensure the confidentiality of email communications and of the ease with which an email which is sent as confidential could be disseminated by its recipient to any number of inappropriate people at the touch of a key. Section Two below specifies some examples of misconduct relating to confidential information and personal data. Employees are advised, however, to consider very carefully the risks of sending confidential information by email, even if they have authority and it is lawful to do so.

(c) Employees should be mindful that non-verbal clues to your meaning are lost in written communication and there is potential for misunderstanding – what's funny to you may appear rude and offensive to a recipient who only has your text to go off.

(d) Employees must avoid typing text wholly in capitals. This is understood as shouting, which is an unacceptable form of communication in the workplace.

(e) Trust your instincts – it's very tempting to reply instantly to emails, but if you've composed a message and 'gut feeling' tells you not to send it, for whatever reason - **don't!** Think about the matter further before committing yourself. In particular, venting rage by email is no more acceptable than shouting in someone's face and sarcastic or angry emails sent in haste are likely to be regretted and may give reasonable grounds for a complaint.

1.8 Employees must be aware of the dangers of inadvertently making or varying contracts over the telephone or by e-mail. Very little is required for a legally binding contract to arise and a quick, apparently informal, phone call or email to a prospective employee or an outside supplier of works, goods or services may result in the inadvertent creation or variation of a contract on terms which are unfavourable to the Council. The Council's contract procedure rules should be followed at all times.. **(Employees should note that nothing in this provision prevents staff making their own personal purchases over the telephone or by using the internet)**.

1.9 You should not give your email password to other people or leave your email/internet access open to others when you are away from your computer.

1.10 Any loss or suspected loss, of authority-provided communication equipment, must be reported as soon as practicable to ICT Services to allow available security measures to be put in place.

1.11 Under the Data Protection Act and the General Data Protection Regulation (GDPR) the Council has a duty to report certain types of personal data breach to the relevant supervisory authority. Under GDPR, it must do this within 72 hours of becoming aware of the breach, where feasible. It is

therefore imperative that all potential breaches are reported to the Executive Director (Legal and Democratic) as soon as they are known.

1.11 Managers have discretion within this policy to determine what is reasonable personal use of Council equipment. This should be considered in the context of the needs of the service, the effect on other employees of their colleagues' actions, and individual employee's personal circumstances. Defining the boundaries of use and misuse of Council equipment may be difficult in some circumstances. It is important that this policy is implemented as consistently as possible and further guidance can be sought from HR to assist employees and managers in this area.

1.12 Misuse of Council communications equipment, whether in the course of an employee's work or personal use is misconduct and is likely to result in disciplinary action under the Council's Disciplinary Procedure either for the misuse itself or for any misconduct which is being perpetrated using Council equipment. In serious cases, it may constitute gross misconduct. If proved, the range of sanctions may include, alongside the normal sanctions open to the Council, that the employee is no longer permitted to make personal use of Council communications equipment.

1.13 If misuse of Council equipment, or misconduct perpetrated using Council equipment, is sufficiently grave as to constitute gross misconduct, the employee may be dismissed, in line with the Disciplinary Procedure.

2. Examples of misconduct

2.1 The following are examples of actions which may lead to disciplinary action:

(a) Personal use of communications equipment **during work time or outside of hours 12 noon – 2pm**, unless permitted in accordance with this policy;
(b) Using equipment in a way which disturbs or causes a nuisance to other employees, or otherwise prevents someone from working;
(c) Using communications equipment to participate in illegal activities;
(d) Using communications equipment or a Council email address in a way which may have the effect of bringing the Council into disrepute or incurring any unauthorised liability whatsoever for the Council or individual concerned;
(e) Making any communications which abuse, threaten, or harass another person or are likely to create or contribute to a hostile working culture or environment or are otherwise anti-social. The Council has a Dignity at Work Policy and if you are unsure what bullying / harassment means, please read the policy;
(f) Employees must not knowingly open a colleague's personal correspondence (including e-mails) without their consent. (Please note that this provision is **not** intended to prejudice the Council's right as employer to monitor communications made on Council communications equipment nor for a manager to access an absent employee's emails to check on outstanding work, if for example they are absent due to unplanned or long-term sickness);
(g) Sending e-mails in another person's name without their consent and without identifying by name the actual sender of the email;
(h) Knowingly downloading from the internet or using or distributing (electronically or otherwise) any intellectual property (e.g. material which is copyright) without proper authorisation and, where appropriate, the Council making payment of a licence fee to the owner of the intellectual property rights;
(i) Making any communications which make any comment, observation or suggestion about another person or company which may be considered to adversely affect or damage their reputation and which may as a consequence expose the Council or the individual to action for slander or libel;
(j) Sending or otherwise distributing personal data processed by the Council about a living individual to a third party without authority **and** if the employee has authority, without satisfying a condition for lawful processing under the Data Protection Act 1998 or related regulations or without the person's consent;
(k) Disclosing any confidential information held by the Council to a third party without authority **and,** if the employee has authority, without the consent of the party to whom the information relates or without an overriding public duty to disclose;
(l) Setting up, without authorisation, any external internet chat room or website using Council equipment. Internal chat rooms may be permitted for business purposes only, but the ICT Section must be

contacted prior to any action to set up an internal chat room being taken;

(m) Participating in the transmission of any junk mail, chain letters or pyramid messages;

(n) On-line gambling;

(o) Any use of the Council's communications equipment to commit a criminal offence;

(p) Knowingly accessing (that is, opening, visiting or looking at a website), or downloading from the internet (that is saving, copying or printing material) or sending, transmitting, disseminating or distributing (electronically or otherwise) any material which is hateful, obscene, pornographic, racist, homophobic or otherwise discriminatory, defamatory, which incites hatred or violence against any person or organisation, or which depicts violence or describes techniques for criminal or terrorist acts or otherwise risks exposing the Council to adverse publicity or bringing the Council into disrepute. **(If you accidentally visit a website which is concerned with any of the above matters, inform ICT and Audit immediately.)**

(q) Any use of the Council's communications equipment which causes serious harassment to another person.

(r) Knowingly accessing data that the Council holds on residents or on individuals without reason. This includes accessing information or records held on friends, neighbours, colleagues or acquaintances.

(s) Accessing and/or amending your own data or records held by the Council such as your Council Tax account, unless specifically authorised to do so (e.g. employee self-service for changes to bank details);

(t) Failing to take reasonable care to protect the Council from viruses, Trojan Horses, malware etc., for example by using a Council PC to charge a mobile phone.

3. Personal use of Council communications equipment

3.1 The Council acknowledges that from time to time most people will need to make arrangements relating to their personal life while they are at work. Personal use by employees of Council communications equipment is permitted by the Council to enable employees to make essential domestic and personal arrangements during working hours. The types of arrangements which employees are likely to have to make during working hours are those related to:

- care of dependents;
- education/care of children;
- healthcare arrangements;
- obtaining goods/services where contact can only be made during office hours;
- household emergencies;
- changes of working arrangements; and
- car repairs/maintenance/services/MOT tests

3.2 Any personal use of Council communications equipment by employees is incidental to the main purpose for which the equipment has been provided to a particular employee and is not to be considered an employment right of that or any employee.

3.3 Heads of Service may withdraw permission to use Council communications equipment from any employee who misuses it.

3.4 Except as otherwise provided in this policy, personal use should take place in the employee's own time, while clocked off, and **only between 12 noon and 2pm**. Where equipment is shared, it may only take place when it is not required by anyone else for a work purpose. Where equipment is shared it is the responsibility of the employee wishing to make personal use to ensure that the equipment is not required by anyone else for a work purpose.

3.5 The Council acknowledges that there may be circumstances when a personal communication during work time cannot be avoided. For example, some service providers may close at lunchtime, or the need to make domestic arrangements may arise during the day. It is the responsibility of each employee only to make personal use of Council equipment in work time if it is essential to do so and that time spent is minimised as much as possible.

3.6 If an employee needs, owing to specific personal circumstances existing at the time, to make frequent or lengthy personal use of communications equipment they must discuss this with their line manager, who may authorise such personal use if the circumstances justify it.

3.7 Employees using Council equipment for personal communications must exercise awareness of other members of staff who may be working around them. Personal business must be conducted in a manner which does not disturb others.

3.8 Where an employee receives an incoming personal communication during work time, they will be expected to exercise reasonable discretion over the time spent dealing with the matter at that point, depending on its urgency and the necessity of dealing with it there and then. Time spent on communications of a social nature which are received in work time must be kept to a minimum and employees should encourage friends and relatives etc. not to make social calls when the employee is likely to be working.

3.9 This policy applies to personal use by employees of portable Council communications equipment away from the work base. Employees who are issued with portable communications equipment are responsible for the proper care and use of that equipment and are issued with a statement of terms and conditions which reflect the applicable requirements of this policy and other Council requirements with regard to the care and use of the equipment.

3.10 Where the Council incurs a cost for the use of communications equipment which can be apportioned to an individual employee, employees will be charged for personal use of Council equipment.

Arrangements for charging are as follows:

(a) Fixed Telephones – employees are expected to pay for calls in accordance with Council procedures which are notified to employees separately from time to time;
(b) E-mails – the Council does not charge employees for use of this system;
(c) Internet use – the Council does not charge employees for use of this system;
(d) Mobile telephones – employees are expected to pay for calls in accordance with Council procedures which are notified to employees separately from time to time; and
(e) Faxes and photocopiers – the Council charges for personal use of fax machines and photocopiers (payment arrangements vary and advice should be sought from the employee's line manager).

4. Employees' use and misuse of own communications equipment

4.1 The provisions in this policy apply equally to employees using their own equipment, e.g. a personal mobile phone, in respect of any communications made during working hours which may:

- bring the Council into disrepute;
- constitute a criminal offence;
- harass or disturb or cause nuisance to another employee;
- create or contribute to a hostile working environment;
- constitute a misuse of the employee's working time; or
- incur any unauthorised liability for the Council or the employee.

4.2 Any such misuse is a disciplinary offence and is likely to result in action being taken against the employee. If the behaviour is sufficiently grave or prolonged to constitute gross misconduct, it may result in dismissal.

4.3 The Council has no powers to intercept or monitor employees' communications made using their own equipment without the user's consent but reserves the right to take any steps which are lawful and proportionate to deal with any suspected breaches of this policy by employees using their own communication equipment.

4.4 Appendix 1 of this Policy gives guidelines to employees on the use of Social Networking sites.

5. Safeguarding Council data on your own equipment

5.1 Whether using Council provided equipment or your own, it is imperative that any Council data held, or program or application allowing you to access Council data, is secure.

5.2 Any security features available on a device, i.e. pin code protection etc., should be activated and used on a regular basis.

5.3 Specifically, with regard to devices accessing a user's Council email account:

- All users must use strong passwords. (At least 8 characters, including at least one number, one special character [$ or % etc.] & one capital letter.)
- Passwords must be protected at all times and must be changed at least every 40 days.
- It is a user's responsibility to prevent their user id and password being used to gain unauthorised access to Council systems.

6. Complaints of bullying or harassment involving communications equipment

6.1 The Dignity at Work Policy is to be found on the Hyntranet or is available from the HR Section, Scaitcliffe House, Ormerod Street.

7. Employees who suspect a colleague is in breach of the Policy

7.1 Employees who have concerns about a colleague's actions in relation to this policy should report these to their line manager. Employees who become aware of more serious potential breaches of the policy are encouraged to take action in accordance with the **Whistleblowing Policy**, which gives details about who to talk to about your concerns.

7.2 The Whistleblowing policy is to be found on the Hyntranet or is available from the HR Section.

7.3 Under no circumstances should employees (this includes managers) carry out their own investigations or surveillance of other employees, unless instructed to do so, as this may prejudice the possibility of the Council taking action and may expose the individual and/or the Council to civil or criminal liability.

8. Monitoring compliance

8.1 Compliance with Council policy is a personal responsibility and it is important that employees are clear about what they can and cannot do using the Council's communications equipment and their own equipment at work. It is also important for managers to be confident that the policy is being complied with and that the Council is not exposed to risk of liability or damage to its systems or reputation.

8.2 All managers are expected to recognise that employees may need to make personal communications during working hours and sometimes during working time. Managers should exercise reasonable judgement at all times about whether an individual employee's use is misuse.

8.3 At the same time, managers must not allow a 'culture' of misuse to develop within their team as this may make it more difficult for the Council to take effective action against any particular employee who is acting in breach of this policy.

8.4 The Council may from time to time undertake monitoring of traffic data on its communications equipment in order to:

- ensure that telephone calls are paid for, and
- enable managers to monitor compliance with this policy

8.5 Monitoring for the purpose of producing bills will be carried out routinely so that bills can be produced periodically.

8.6 Monitoring of traffic data for the purposes of monitoring compliance with the policy will be carried out by the ICT Section:

(a) according to a programme of routine review by Internal Audit under the Audit Plan;
(b) at the request of a member of the Council's Management Team, the Head of Legal Services, the Monitoring Officer (if not one of the officers previously mentioned) or the Head of Audit & Investigations, where there is reasonable suspicion of possible misuse of the Council's communications equipment; or

(c) at the initiation of the ICT Service Manager to safeguard Council ICT systems in line with the ICT Security Standards and Guidance

8.7 Monitoring of traffic data may indicate breaches of this policy which require further investigation, for example, access to internet sites in breach of this policy.

8.8 The Council will make all reasonable efforts to notify anyone who communicates with the Council using its telecommunications systems that monitoring may take place.

Appendix 1: Social Media Guidelines

1. Introduction

1.1 Social media is any 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, Myspace, Reddit, Twitter and LinkedIn. Social media also covers video and image sharing and blogging websites such as YouTube, Instagram, Snapchat, 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. The Communications Policy applies in relation to any social media that employees may use.

1.2 Social media presents new and interesting opportunities for people and organisations to reach out to others. It allows anyone with a computer and internet connection to publish opinion and information, and to listen to and engage with those who read it.

1.3 However, there are risks attached to the use of social media and these guidelines are intended to help protect the Council and also individual employees.

1.4 Any information or comments published on any site (internal or external):

- may stay public for a long time;
- can be republished on other websites;
- can be copied, used and amended by others;
- may be perceived by others as offensive, even if this was not intended;
- could be changed to misrepresent what has been said; and
- can attract comments and interest from other people.

1.5 Things which are written, shown or received via social networking sites could be made available, intentionally or otherwise, to an audience wider than that originally intended.

1.6 It is therefore important that users of social media understand the pitfalls as well as the benefits of the technology. Employees have a right to a personal life, and provided they do not breach reasonable conduct guidelines, the Council will respect this. These guidelines suggest actions which may avoid employee relations problems.

1.7 The TUC referred to the UK's Facebook users 'as 3.5 million HR accidents waiting to happen'. There are numerous examples of issues concerning the use of social networking sites by employees, some of which are given below.

- Directory enquiries group 118 118 discovered workers were making comments about callers they had dealt with. The company investigated the workers who were involved and disciplinary proceedings followed.
- Virgin Atlantic dismissed 13 cabin crew after disciplinary proceedings concerning messages on Facebook referring to passengers as 'chavs' and making jokes about them.
- An employee was dismissed after less than a month in her job following her comments on a networking site on how boring her job was.
- A prison officer was dismissed for gross misconduct after befriending former and current inmates on Facebook.

2. Authorised use for work purposes

2.1 A limited number of employees may be authorised to use social media as part of their work for Hyndburn Borough Council. Although access may therefore be granted to such websites using Council equipment, permission is **not** given for personal use.

2.2 Employees must use council facilities appropriately: if you use a council-provided blog site or social networking area, any posts you make will be viewed as made in your official capacity. You should also be aware that by publishing information that you could not have accessed without your position as an officer, you may be seen as acting in your official capacity.

2.3 Other than for these authorised employees, social networking sites are blocked from Council computers and such sites should not be accessed using Council equipment. Employers using such sites for work purposes must ensure that their manager is aware of this activity.

2.4 Employees should not use their work e-mail address to use social networking sites, e.g. to set up a profile.

3. Recruitment and selection

3.1 Social networking sites will not be searched in order to obtain information to inform decisions on recruitment and selection. There is a danger that the use of information obtained in this way could lead to perceptions and challenges of unfairness or discrimination.

4. Social Networking and Personal Conduct

4.1 If employees use social media for their own personal use or within their role there is a requirement to stay within the law at all times, and to be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line just as in any other media.

4.2 Colleagues and customers of employees may see employees' online information. Whether individuals identify themselves as an employee of the Council or not, it may be advisable to think carefully about how much personal information is made public to ensure that the information posted reflects how an individual wants to be seen both personally and professionally.

4.3 Employees should be aware that even if they are not listed as Council employees on one social networking site (e.g. Facebook), they may be on another (e.g. LinkedIn) and this can allow others to make that link.

4.4 Employees may also wish to consider whether they are seen to be, or give the impression that they are acting in their official capacity as a Council officer.

4.5 Employees should take care not allow their interaction on these websites or blogs to damage working relationships with or between employees, elected members, customers, or contractors, for example by criticising or arguing with them or using abusive or threatening language. This can include reacting to offensive posts made by other people in a way that indicates agreement – for example by "liking" or retweeting a critical post.

4.5 Legal issues

a) **Breach of contract**

There is an implied term of mutual trust and confidence between employer and employee in all employment contracts. Disclosing confidential information or making or participating in a very negative and damaging posting or communication about the employer may entitle the employer to state that this term has been broken and warrant the employee's dismissal in line with the disciplinary procedure.

b) **Defamation**

If defamatory material is posted on a social networking site, defamation claims may arise against the employee.

c) **Discrimination**

Difficulties arise if information from networking sites is used to make discriminatory decisions, for example to refuse a job on grounds of race, sexual orientation, religion or age. Employers must not make a decision on such a basis otherwise they are exposed to expensive discrimination claims. Also only a minority of candidates will have profiles on social networking sites and using information from this source can give an unfair advantage or disadvantage to certain candidates possible discriminating against younger people who use the sites more.

Other discrimination claims may arise if employees post discriminatory material about other employees which could amount to bullying or harassment.

d) **Whistleblowing**

Nothing in this policy should be seen to restrict the use of the Council's Whistleblowing Policy. Whistleblowing is the term used when someone who works for the Council raises a reasonable and genuine concern about a possible fraud, crime, danger or other serious risk that could threaten the public, their colleagues or the reputation of the Council.

e) **Health and safety**

In 2007 a UK based employer saw internet video clips of employees performing stunts wearing its uniform. An employer who discovers information like this should follow the disciplinary procedure to investigate the possibility of a breach of health and safety legislation on the part of the employee. If an employer is aware of this and fails to investigate there may be liability for personal injuries in the law of negligence.

4.6 Avoiding problems

These Guidelines give suggestions to consider in relation to their personal use of social networking sites. Employees are entitled to a reasonable degree of privacy but also have some responsibility for and influence over the content of information on their personal pages / sites. Factors such as the nature of the person's job (e.g. seniority, political restriction) may influence how an employee wishes to try and manage their online presence and these factors will influence how the Council may respond.

Things to consider

- Look at the privacy settings for your blog or networking site. For instance, on Facebook, you have the option to only allow "friends" to see your posts. It is more difficult to argue that a profile which is open to everyone is not in the public domain.
- If others post defamatory or obscene statements / pictures etc. on your blog or page, or you "like" or otherwise comment on or share their posts, be aware that this might lead some people to believe that you condone such views.
- Please note that guidance given to Hyndburn's councillors suggest that they should not request or accept a Hyndburn BC employee as a "friend" on a social networking site.
- If you make derogatory remarks about the Council, colleagues or customers, you risk this becoming a work issue.
- Consider whether you want to include details of your employer / workplace in your personal details.