# Internet, Use of Email and Social Media Policy

| | | | |
|---|---|---|---|
| **Author:** | Sue Leppington, Director of finance and central services | **Approved by:** | Governance, Ethics, Remuneration and Nominations Committee |
| **Audience** | All employees including agency workers, board members, contactors and volunteers | **Approval date:** | October 2024 |
| **Date effective from:** | October 2024 | **Review date:** | October, 2026 |

## 1. Introduction

To operate effectively, organisations need to communicate appropriately.

It is important to ensure that we treat everyone, internally and externally, both professionally and courteously. This policy is to be regarded as a code of conduct on e-mail, internet and social media usage and all aspects of communication.

It applies to all employees including agency workers, board members, contractors, volunteers, and any other person working with CIH.

Any breach of this policy will be considered under the Disciplinary procedures of CIH.

Policy Principles:

Written communication

- All written communication should use language that is easy to understand, free from unnecessary jargon, be professional, polite and spell checked.

E-mail and internet use

- CIH has invested in the necessary resources to provide employees with the facility to use e-mail and to access the Internet which is beneficial in enabling them to undertake their duties more effectively. These facilities may only be used for business purposes except in certain circumstances.
- We recognise and embrace the benefits and opportunities that social media can bring as a communication, and engagement tool. We want to use social media to maximum effect, whilst protecting CIH, and those using our services.
- We want to prevent any legal issues that may arise through the use of these tools.

This policy should be read in conjunction with other relevant policies, including Code of Conduct, Complaints, Confidentiality, Cyber Security, Data Protection, Dignity at Work, Privacy Notices, and Safeguarding.

## 2. Email

Email should normally only be used to communicate internally with colleagues and externally to clients or relevant organisations, on business related issues.

Personal messages should be kept to a minimum. Once you leave CIH, your mailbox will be wiped. The mailing of sexually explicit or otherwise offensive material, either internally or externally will be investigated under the Disciplinary policy and may be found to be gross misconduct.

Usage expectations:

- All colleagues should ensure that the automatic 'out of office' assistant/response and/or message forwarding facilities are used to cover absences. They should cover when you will be away and when you will return to the office and who to contact if there is an urgent matter.
- No e-mail containing any references to other individuals which might be construed as libellous, or which might be regarded as harassing or insulting, may be sent using CIH's system.
- Complaints about the performance, or service, of other organisations or individuals must be made informally first and then followed up in a formal letter, as is reasonable practice and in consultation with your line manager.
- CIH recognises that it is not always possible to control incoming mail. Any material received which would be considered as non-businesslike, sexually explicit or offensive should be reported to the IT department and/or HR who will inform your line manager.
- E-mail may be used for the despatch of formal documents such as contracts or proposals. You should consider confidentiality requirements (i.e. use of passwords) and that documents issued this way are just as legally binding as those sent conventionally. You should ensure you have the authority to send such documents and if you are unsure, check with your line manager before sending.
- E-mails which are sent to recipients outside CIH should be composed in a professional and businesslike manner.
- Unsolicited e-mails must not be sent at any time. Any 'junk' mail received should be deleted.
- It is a disciplinary offence to access another individuals' e-mail facility by using their password and you should never share your passwords with anyone, internally or externally.
- Employees should exercise extreme care when receiving e-mails with attachments from third parties, particularly unidentified third parties, as these may contain viruses.
- Any accidental sending of an email containing personal information (name, email address, membership number etc) to an unintended recipient should be reported to the data protection officer as a data breach in accordance with our Data Protection policy and they will advise you of the necessary actions to take.
- You should inform your line manager if training is required to ensure adherence to this policy.
- Computers, networks, e-mail systems etc are the property of CIH. Emails are not the property of colleagues and as such there can be no expectation of privacy.

## 3. Internet

Accessing the Internet is a legitimate and useful way to search or research on behalf of CIH. CIH also accepts that employees may find it convenient to browse the Web for their own personal reasons during their own time (e.g. lunch break).

Usage Expectations:

- Searches of the internet should only be undertaken with the safe search function enabled to restrict explicit materials.

- You should not access, view, receive, download, send or store material from sites such as those relating to pornography, racism, terrorism, cults, hate speech, illegal drugs, or other inappropriate sites. To do so may be considered an act of gross misconduct. The only possible exceptions to this are for employees who need to access such sites in relation to work. Visits to such sites however should be limited strictly to work-related issues and you should inform your line manager ahead of time to avoid any misunderstanding.
- If you decide to buy anything over the Internet you should ensure that, if you give credit card details or other sensitive information, you have a secure connection. CIH will not be liable for any personal information that may be stolen.
- Goods may be received on CIH premises, but this should be kept to a minimum and if in any way it interferes with the smooth running of the office, employees may be asked to cease the practice.
- You should not generally join any mailing lists or solicit any information on the Internet unless there is a work-related need to do so. Should you wish to take part in such activities in a private capacity, you should do this outside of working hours and use your personal email address.
- It is forbidden to place any CIH material on any publicly accessible website unless this is part of your job role.
- CIH reserves the right to view and monitor all e-mail and internet access.
- The list of examples above is not exhaustive. Depending on the circumstances of each case, any use of ICT deemed to be unauthorised, to bring CIH into disrepute or deemed to be in any way unwelcomed by CIH will result in disciplinary action, which may lead to dismissal. Misuse amounting to criminal conduct will be reported to the police.

## 4. Social Media

For the purposes of this policy, social media is defined as a type of interactive, online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social media forums, social apps, blogs, videos and image sharing websites, and instant messaging apps including, but not limited to, X, Facebook, Instagram, TikTok, YouTube, LinkedIn, and WhatsApp. Posting online will leave a digital footprint which can be referred to in years to come. It's really important that you think carefully about what you engage with and how you engage with it.

An employee's behaviour on any social networking or other internet site must be consistent with the behaviour required of employees generally. Where it is possible for users of a social media site to ascertain who you work for, then you should take particular care not to behave in a way which reflects badly on CIH.

You must avoid making any social media communications that could damage our business interests or reputation, even indirectly. You must not use social media to:

- defame or disparage us, our colleagues or any client or other third party;
- harass (including sexually harass), bully or unlawfully discriminate against colleagues, clients or other third parties;
- make false or misleading statements; or
- impersonate colleagues or third parties.

Because social media interactions can be copied and widely disseminated in a way that you may not be able to control, CIH will take a particularly serious view of any misconduct that occurs through the use of social media.

You should make it clear in social media postings, or on your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal email address. Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

You must not operate a social media account or profile or express an opinion that purports to be operated/made on behalf of CIH without express permission to do so from your line manager. You must not comment on social media about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

You are not permitted to add business contacts made during the course of your employment to **personal** social networking accounts.

You should not attempt to access social networking sites, such as Facebook/X (formerly known as Twitter) or similar on Company computers unless done in the course of your role.

Regardless of which social networks employees and volunteers are using, following these usage expectations will help to avoid common pitfalls:

- If posting as part of your role, only post in line with our brand guidelines – these can be found on the shared drive under Brand Assets.
- Ensure you have permission in writing to use third party logos, brand names, trademarks, or slogans. Remain aware of copyright when using images, video, music of other media.
- Maintain confidentiality, don't cite or quote colleagues, volunteers, partners, or individuals without their permission in writing to do so.
- Don't share internal or confidential information about CIH or an individual relating to CIH without prior approval.
- Fact check and reference all sources in accordance with copyright law before posting
- Don't share inappropriate content, make sure you read the post or article fully before posting.
- Be thoughtful, polite and ensure responses are reviewed regularly.
- Beware of over-promising. Don't make a specific commitment before checking we can deliver it.
- Handle complex queries through other channels.
- Know the social network – ensure you are familiar with any T&Cs or requirements before using it.
- Regularly check your privacy settings.
- Regularly update your passwords and do not share them with anyone.
- Be vigilant – check for imposter social media accounts.
- You must not post any political campaigning material, nor encourage voting one way or another. Personal political views must not be shared via CIH accounts.
- If at all unsure, don't post.

Any misuse of social media that you see should be reported to your manager.

Breach of this policy may result in disciplinary action up to and including dismissal. You may be required to remove any social media content that we consider constitutes a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

## 5. The Media

The press, TV and radio can be powerful friends for organisations like CIH and the people we exist to help. But they also have their own agenda which may conflict with our own.

For this reason, we need to handle our contact with the media with great care.

Enquiries and requests for information or comment from the media fall into three main categories:

i) Enquiries about specific incidents or individual people
ii) Requests for comment on general housing issues
iii) Requests for factual and statistical information

For all of the above scenarios, you should not give an opinion or comment, and refer the matter to either your line manager, the Policy and Public Affairs team and / or the Chief Executive Officer.

If you have any concerns about the application of this policy or believe that you or someone else may have fallen foul of it, please speak to your line manager or HR.