****

ASHLEY HIGH SCHOOL

Internet Access/Acceptable Use policy

Reviewed: September 2023

Next review: September 2025

Reviewed by: A. Ivins

**ASHLEY HIGH SCHOOL**

**Acceptable Use Policy**

**Internet, E-mail, Fax, Telephone communication, Printing Facilities and Mobile Devices**

**Updated: September 2023**

**1. Introduction**

The Acceptable Use Policy provides Halton Borough Council staff with managerial instructions on the acceptable use of Council facilities, including the use of the Internet, e-mail, telephones, faxes, Printing facilities and communication software products including Microsoft Lync for council or personal use.

The Acceptable Use Policy also provides staff with management instructions on the acceptable use of non-council ICT equipment within works time.

The Internet and e-mail facilities are provided to employees of Halton Borough Council in order to support the goals and objectives of the Council, and the professional, efficient and effective use of these facilities is expected.

The Council and all of its employees must demonstrate and comply with a high degree of public accountability. This Policy has been developed with that in mind. The Council’s assets are public property, and management has a duty to ensure that the use of those assets is in line with the public interest.

All use of Council assets must:-

* Be acceptable
* Be auditable
* Be compliant with legislation
* Not create unnecessary business risk to Halton Borough Council
* Be authorised

**2. Coverage of Policy**

This Policy applies to all Halton Borough Council employees, agency workers, external contractors, casual workers, volunteers, employees from other organisations using Halton Borough Council equipment, elected members and those working on secondment (referred to herein as “staff”).

The Policy covers the use of all Information Communication Technology (ICT) equipment – all Personal Computers, Laptops, tablet devices, phones, fax machines, Multi-Functional devices, printers and terminals as well as mobile devices. Mobile devices as specified within this Policy refer to any mobile device including but not limited to Mobile phones, Tablet Devices, Portable Computers, iPhones and other Personal Digital Equipment (e.g. PDAs).

The Policy also covers the use of all communication sharing tools which include but are not limited to; Lync (including Instant Messaging) SharePoint and the Intranet.

Within this Policy clocked on and clocked off refers to being within works time or outside of works time.

Throughout this policy the term ‘call’ refers to calls made from mobile devices, landlines and Communication software products such as Microsoft Lync. This includes calls made directly from ICT equipment via a handset and/or headset.

**3. Code of Conduct**

The most important message to understand is that all activity on computers and communication devices is logged and retained – both on the device/network that is being used as well as by a third party. (E.g. Internet Website/e-mail recipient).

Everything that is done on Halton Borough Council’s network with Halton Council user ID’s and e-mail addresses reflects on the Council.

**3.1 Use of e-mail, Internet, Printing facilities, telephone communication systems and communication sharing tools**

Authorised users of Internet/e-mail, telephone communication systems and communication sharing tools may use Halton Borough Council’s computer equipment and council-provided software as long as ALL the following conditions are adhered to:

3.1.1 Personal use of Halton Borough Council’s ICT equipment within works time, without explicit management consent is not authorised and strictly forbidden and may lead to disciplinary action being undertaken.

3.1.2 Staff must NOT use their Halton Borough Council e-mail address for ANY personal use regardless of this being in works time or not. This is strictly forbidden.

3.1.3 Reasonable personal use of equipment (excluding the use of Halton Borough Council e-mail) may be permitted when the authorised user has clocked out if on a lunch break, flexitime or otherwise their own time – again, subject to management discretion.

3.1.4 Staff must be aware that any personal e-mail address used to e-mail the council will be stored on the Council’s servers including the contents of the emails. Staff members who directly e-mail using their personal e-mail account to a Council e-mail account whom are already covered by this Policy will be treated just the same as if the e-mail had originated from a Council address, regardless of whether the individual was clocked on or off.

Note: Whilst the use of a Halton Borough Council e-mail address provides an official record of Council activity, there is also a requirement on individuals to ensure that any content that resides on the Council’s infrastructure from an e-mail address that is operated or managed by themselves complies with this Acceptable Use Policy, and it is therefore included in the scope of this document. E-mails from personal addresses, while they may not be created on Halton equipment can and do form part of the Council’s records and maybe subject to disclosure under FOI, and/or SAR.

The reason for this requirement is by storing any e-mail on the Council’s servers, even though it isn’t from a Council address may be subject to disclosure under FOI, and/or SAR.

3.1.5 When using the Internet and communication sharing tools such as fax facilities for personal reasons (with explicit management consent only) staff are reminded that they are still using an address which identifies them as an employee of Halton Borough Council, and therefore could be judged by recipients to be acting on behalf of Halton Council. All users of e-mail must ensure that anything that is communicated within e-mail, whether personal (which is prohibited) or not does not bring the Council into disrepute.

3.1.6 All PC usage, e-mails, sites visited via the Internet, the use of communication sharing tools whether for Council business, or personal use will be logged and kept by Halton Borough Council. These logs are available to Management and Internal Audit and can be audited at any time.

3.1.7 Council equipment must not be used to send e-mails, across Internet sites (personal or business), add information to communication sharing tools including instant messaging that for example contain or have attachments that contain: defamatory, offensive or harassing language, fraudulent material; sexually explicit images or language; material that infringes copyright or other intellectual property rights of third-parties or offensive cartoons or jokes or otherwise involve unlawful or wrongful conduct. For e.g. comments and language used on social networking sites.

3.1.8 Staff must not post or Tweet negative comments in personal or works time (personal or council owned equipment) about your employer, colleagues and members of the public or other work related organisations. Halton Borough Council’s relationships with clients, customers and partners are valuable assets that can be damaged through a comment.

3.1.9 Staff must not use instant messaging to make negative comments in personal or works time about your employer, colleagues and members of the public or other work related organisations. Instant messaging is a tool that should be used for work purposes.

For further advice on how to use the Internet securely (on a professional and personal level) visit the Information Commissioner’s Office at:

<http://www.ico.gov.uk/forthepublic/topicspecificguides/socialnetworking.aspx>

Halton Borough Council has also produced further guidance specifically for staff using social networking sites as below:

Appendix A – Social Networking Guidance is available at the following link:

<http://hbc/teams/ITSECPOL/Shared%20Documents%202/Appendix%20A%20-%20Social%20Networking%20Guidance.pdf>

There is also further guidance on social media for Halton Borough Council business use which is available within the “Social Media Policy” or contact research@halton.gov.uk.

For further guidance on how to use Halton Borough Council e-mail securely and professionally visit the guidance as below:

Appendix B – E-mail Good Practice Guidance is available at the following link:

<http://hbc/teams/ITSECPOL/Shared%20Documents%202/Appendix%20B%20-%20Email%20Good%20Practice%20Guidance.pdf>

If a user inadvertently accesses an unauthorised site, or receives an e-mail or instant message that contains inappropriate content they must report this to their Line Manager and the ICT Service Desk immediately.

3.1.10 The Council’s ICT equipment, Internet, e-mail, telephones, communication sharing tools and fax facilities must not be used in connection with any personal business activity or other paid employment.

3.1.11 Users must not plug in any non-Halton Borough Council equipment into the Council network. Equipment must be owned or managed by the Council to access the Council network. Note: Owned machines are devices purchased by the Council. Managed devices are devices that are registered and locked down by the Council to meet the Council’s security requirements.

3.1.12 The personal use of Internet and other communication sharing tools, whilst clocked out (excluding e-mail) at Halton Borough Council is a privilege and not a right. The Council reserves the right to withdraw or limit such facilities either generally or to an individual.

3.1.13 Storage of personal documents on Halton Borough Council’s equipment must be kept to an absolute minimum. Transferring personal documents to Council equipment could lead to the introduction of viruses and also could lead to capacity issues.

3.1.14 It is accepted that, in certain circumstances, it may be necessary to use private e-mail for public authority business. Private e-mail must not be used for transferring/storing personal or sensitive information. Non-personal/non-sensitive information e-mails that are used within a private e-mail should be copied to the person’s Halton Borough Council e-mail address also.

3.1.15 Users must not upload, download or copy any copyrighted material or software (or non-work related non-copyright material) without the express prior written permission of their Line Manager and ICT Security Management – this includes MP3, audio and video content that has not been purchased by the Council.

3.1.16 Users must not, without proper authority reveal or publicise confidential or proprietary information when using any electronic service provided by the Council.

3.1.17 Users must not enter into contracts or other legal commitments on behalf of Halton Borough Council except with the prior specific written permission of their Line Manager. An e-mail is considered an official record of the Council and therefore can be enforceable in law as a contract.

3.1.18 Halton Borough Council will assist the relevant authorities in taking action against any employee who commits an unlawful act whilst using the Council’s computer facilities. Suspected criminal activity may be reported to the Police.

3.1.19 All digital content, created or stored on Halton Borough Council equipment are deemed to be the property of the Council. Personal e-mails or other documents which are kept on Council equipment may be required to be made available to third parties. This can arise under the Freedom of Information Act 2000, Data Protection Act 1998, and other legislation or under Court order or other legal duty.

3.1.20 Business e-mails must clearly indicate the following at the end of the message: Employee Name, Job Title, Department, Halton Borough Council, Telephone Number, (if available Direct Dial number), Extension and Web Address.

3.1.21 E-mails from unknown sources or which may appear suspicious must not be opened. Software received via e-mail must not be installed. Users must consult the ICT Service Desk for advice if e-mails or software is received from an unknown source or which is otherwise suspicious. Users must not circulate ‘spam’ or junk e-mail to other users. All such mail must be forwarded to the ‘spam’ e-mail account. Joke e-mails (visual or text) must not be circulated.

3.1.22 E-mails are formal documents and must not contain remarks that may be embarrassing or sensitive to Halton Borough Council, its elected or other Members, its employees, its volunteers, contractors or agency workers or the general public.

3.1.23 Users must not disclose confidential information relating to Council business, speak on the Council’s behalf or make comments regarding staff or members of the public on social networking sites or other sites without management authority.

3.1.24 It is illegal to send personal or sensitive information over unencrypted networks (such as external e-mail). All personal or sensitive information can only be sent over secure connections. Staff should contact the ICT Service Desk for advice on acceptable methods of transferring information.

3.1.25 The Council’s ICT network and Internet access is a shared resource. If a user generates excessive network traffic, ICT services will take action to ensure that the network continues to provide an acceptable level of response across the Council. This may involve restricting access to websites (e.g. media streaming) or disabling an individual user connection.

3.1.26 Users must NOT use their Halton Borough Council e-mail address for subscribing to any non-work related websites, electronic services or social media sites.

3.1.27 Any use of the Council’s Staff Forum shall be in accordance with the instructions provided on the Intranet.

3.1.28 Multi-functional devices are not to be used to e-mail external non-council addresses. Users must e-mail themselves from the Multi-Functional devices if required and then send the e-mail from the users e-mail account. The e-mail must be encrypted if this contains personal/sensitive information.

3.1.29 Personal use of Halton Borough Council’s printing/scanning facilities within works or non-works time, without explicit management consent is not authorised and strictly forbidden.

3.1.30 Users must not use their e-mail system as an electronic document management system. Documents must be stored according to the “Records Retention Policy” and all e-mail is automatically archived.

3.1.31 Users must not deliberately corrupt or destroy other user’s data.

3.1.32 Users must inform the ICT Service Desk immediately if they think they have access to any information or information processing facilities which they don’t think they should have for example, personal/sensitive information within another user’s calendar or access to a mailbox. Users should report the issue and not view the information.

3.1.33 Users must not deliberately delete required data before leaving the Council as an employee.

**3.2 Telecommunications (including Mobile devices, Landlines and other communication sharing tools such as Lync)**

3.2.2 Communications equipment must not be moved, unplugged or switched off except with the express prior written permission of the ICT Service Desk. This does not include headsets and/or handsets that are attached to equipment.

3.2.3 All incoming and outgoing telephone calls are logged and provide usage statistics for each Council telephone extension.

3.2.4 Settings on telephones must not be altered as this could cause a failure for the telephone to ring. Proper use of divert or follow me facilities is permitted.

3.2.5 Where Voice-Mail facilities have been authorised for business purposes they must not be used as an alternative to answering the telephone. Voice Mailboxes must be checked on a regular basis.

3.2.6 The Council’s ICT facilities are provided to deliver high quality and efficient services. The Microsoft Lync unified communications services should be used to provide maximum efficiency and availability of Council staff and accordingly, the features and facilities must not be misused or abused.

**3.3 Personal use of Telephones and Fax Machines at work**

3.3.1 Personal or work mobile devices must not be used to access the Internet for personal use during working time. This includes accessing social networking sites, private e-mail addresses or viewing ANY Internet sites from the mobile device.

3.3.2 The use of the Council telephone system for the making of personal calls or the sending of personal faxes must not take place unless in exceptional or emergency situations. Where a public phone is provided the employee must use that facility.

3.3.3 Personal incoming calls (by landline or mobile) or faxes with the exception of emergencies whilst at work should be discouraged and where unavoidable must be kept to a minimum.

3.3.4 Personal Mobile devices such as Mobile phones must be set on discreet mode (or equivalent).

3.3.5 Users must not make personal calls or send faxes when clocked in barring emergency situations. Users can only make personal phone calls in emergency situations with express permission from their Line Manager.

3.3.6 Mobile devices shall only be used at work in accordance with instructions issued by the Employer.

**4. Disclaimer**

Halton Borough Council does not guarantee the security of ANY information that users may enter while making permitted personal use of Council equipment. The Council disclaims ALL liability that may arise from loss or harm suffered by a user as a result of that information being disclosed or being used so as to cause loss to the user. The Council disclaims ALL liability for such losses and any employee using Council equipment for permitted private purposes does on the basis of having agreed this disclaimer of liability.

The Council disclaims ALL liability that may arise from loss or harm suffered by a user as a result of a financial transaction whilst using Halton Borough Council’s equipment.

**5. Monitoring**

Halton Borough Council accepts that the use of Internet, e-mail, telephones, communication sharing tools including instant messaging, fax machines and printers/MFD’s is a valuable business tool. However, misuse of such facilities can have a negative impact upon employee productivity and the reputation of the Organisation.

In addition, all of Halton Borough Council’s Internet, e-mail, telephones, communication sharing tools and fax resources are provided for business purposes. Therefore, the Council maintains the right to examine any systems and inspect any data recorded in those systems. This is also to comply with the “Prevent Duty Guidance for England and Wales (2015)” in terms of trying to limit access to terrorist and extremist material.

In order to ensure compliance with this policy, Halton Borough Council also reserves the right to use monitoring software in order to check upon the use and content of such resources. Internet, e-mail, communication sharing tools usage reports will be distributed to Divisional Managers on a regular basis and may result in disciplinary proceedings.

These communications may be intercepted or recorded by the Council as an aspect of monitoring (or recording) business communications for any one of the following purposes:-

* To establish the existence of facts.
* To check that the business is complying with regulatory or self-regulatory procedures.
* To check the standards that workers are achieving.
* To show the standards workers ought to achieve.
* To prevent or detect crime.
* To investigate or detect unauthorised use.
* To ensure the security of the system and its effective operation.

Compliance will also be monitored via regular audits as part of the audit programme.

The monitoring of communications will take place in accordance to the Telecommunications (Lawful business practice) (Interception of communications) Regulations 2000 and there is also a Halton Borough Council RIPA Policy in place to be adhered to.

**6. Security Issues**

Information that needs to be accessible to other employees and your Line Manager whilst you are out of the office MUST be stored on a secure shared area and not directly on your equipment. Personal/Sensitive information should be stored in secure areas that ONLY relevant employees have access to or MUST be password protected.

Passwords must NOT be disclosed nor shall individuals be permitted access to others’ ICT equipment and systems except with the prior approval of the relevant Divisional Manager or above. Disclosed passwords must be changed as soon as operationally possible as stated within the Standing Orders Relating to Information and Communications Technology Policy.

**7. Consequences of non-compliance**

The Acceptable Use Policy is consistent with statutory duties and the common law. Failure to comply with the Acceptable Use Policy may result in disciplinary action being undertaken according to Halton Borough Council’s Disciplinary Procedure.

Staff must also be aware that disciplinary action may be undertaken if an employee for example comments on a social networking site outside of works time using their own ICT equipment or Halton Borough Council’s equipment about another member of staff. The Disciplinary procedure will be enforced if comments are deemed to be inappropriate or have breached confidentiality.

**8. Accessibility**

If the Acceptable Use Policy is required in different formats such as large print, audio tape and Braille please go to the following link for information:

<http://intranet/Pages/Interpretation%20and%20Translation-Guidance.aspx>

**9. Supporting Documentation**

This policy has been based on ISO 27001-2013 Information Technology – Security Techniques – Information Security Management Systems Requirements and must be read with the following supporting documentation:

* Standing Orders Relating to ICT
* Personal Commitment Statement
* Information Governance Handbook
* Council Constitution
* Disciplinary Procedure
* Records Retention Policy
* Regulation of Investigatory Powers (RIPA) Policy

In the event of any conflict with the Constitution or the above procedures, then the Constitution prevails.