HARTLEPOOL
BOROUGH COUNCIL

Policy Document

Internet Acceptable Usage Policy V4.0

February 2022

Document Control

Organisation	Hartlepool Borough Council
Title	Internet Acceptable Usage Policy
Author	Jeff Mason
Date created	June 2010
Next review date	March 2023

Revision History

Revision Date	Reviser	Version	Description of Revision
June 10	Alison Oxley	1	
Sept 11	Jeff Mason	2	Revision with Information Governance Group comments
Mar 15	Paul Diaz	3	Added comment re social media updated Information group membership
Feb 17	S Russell	3.1	Minor format changes
Mar 20	IG Group	3.2	Minor changes
May 21	Chris Pendlington	3.3	Minor changes
Feb 22	Kay Forgie	4.0	Section 6.5 amended to exempt work related Lync & MS Teams messaging. Section 10 HBC Code of Conduct added

Document Approvals

Version	Approved by	Date approved
3.1	Information Governance Group	17 February 2017
3.2	Information Governance Group	11th March 2020
3.2	C Little, Director of Finance & Policy (SIRO)	20th July 2020
3.3	C Little, Director of Resources and Development (SIRO)	7th June 2021
4.0	C Little, Director of Resources and Development (SIRO)	19th May 2022

1 Policy Statement

Hartlepool Borough Council (the Council) will ensure all users of Council provided internet facilities are made aware of the acceptable use of such facilities. This will be achieved by publicising the policy and ensuring users have verified their understanding and acceptance of it. Appropriate training and guidance will be provided as required and members of the Information Governance group (see Appendix 1) along with Corporate ICT Team (CICT) are available to provide advice on the policy.

2 Purpose

The purpose of this Policy is to outline the responsibilities of all users of Council internet facilities and set out what is and is not acceptable use. The policy:-

- Provides guidance on expected working practice.
- Highlights issues affecting the use of internet.
- Describes the standards that users must maintain.
- States the actions that may be taken to monitor the effectiveness of this policy.
- Warns users about the consequences of inappropriate use of the internet.

It is recognised that it is impossible to define precise rules covering all Internet activity and adherence should be undertaken within the spirit of the policy to ensure productive use of the facility is made.

3 Scope

This policy is intended for all Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of the Council's internet facility.

The use of the internet facility will be permitted only by staff who have confirmed in writing that they accept and agree to abide by the terms of this policy.

The use of the internet facility by staff that have not agreed to this policy will be regarded as a disciplinary offence.

4 Definition

This Internet Acceptable Usage Policy should be applied at all times whenever using the Council provided Internet facility. This includes access via desktop computer or by way of any remote / mobile device (including mobile phones) equipped with internet access capability.

5 Risks

The Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business and by the use of internet facilities.

This policy aims to mitigate associated risks including the following:

- Inappropriate use of the internet including that which results in legal action, loss of reputation to the Council or other adverse publicity.
- Time wasting by inappropriate and unauthorised use.
- Congestion and disruption to the network and systems arising from unauthorised downloading of files or software.
- Downloading viruses and ransomware from the use of personal email (yahoo, gmail, outlook etc.).

- Failure to report information security incidents immediately.

6 Applying the Policy

6.1 What is the purpose of providing the internet service?

The internet service is primarily provided to give Council employees, Councillors and other approved users:

- Access to information that is pertinent to fulfilling the Council's business obligations.
- The capability to post updates to Council owned and/or maintained web sites.
- The capability to upload information to Government and other appropriate web sites.
- The ability to interact with customers and conduct transactional business.
- An electronic commerce facility.

6.2 Personal Use of the Council's Internet Facility

The Internet facility is primarily made available for the business purposes of the Council. However, at the discretion of your line manager, and provided it does not interfere with your work, the Council permits a certain amount of personal use of the Internet.

This is limited to a **maximum of 90 minutes per day** in your own time, outside of working hours (for example prior to work, during your lunch-break and following work) and is subject to the same standards as business use.

The Council is not, however, responsible for any personal transactions you enter into, for example in respect of the quality, delivery or loss of items ordered. Use of the Internet for personal use is done so at the user's own risk.

You must accept responsibility for, and keep the Council protected against, any claims, damages, losses or the like which might arise from your transaction - for example in relation to payment for the items or any personal injury or damage to property they might cause.

If you purchase personal goods or services via the Council's Internet service you are responsible for ensuring that the information you provide shows that the transaction is being entered into by you personally and not on behalf of the Council.

You should ensure that personal goods and services purchased are not delivered to Council property. Rather, they should be delivered to your home or to another personal address.

Similarly, you should not use your council email address to purchase goods / register to websites as such transactions are personal to you and have no connection with the council. In addition receiving such communications may cause additional 'spam' traffic to council email addresses with the associated risks such unsolicited material may bring.

If you are in any doubt about how you may make personal use of the Council's Internet service you are advised not to do so until you have sought advice from your Information Governance Group Representative.

When accessing websites and email for personal use then users must not click on links or websites unless they are certain they are legitimate.

Any user who clicks on a link which results in unexpected results should report this immediately to CICT.

All personal usage must be in accordance with this policy. Your computer and any data held on it are the property of Hartlepool Borough Council and may be accessed at any time by the Council to ensure compliance with all its statutory, regulatory and internal policy requirements.

6.3 Personal Conduct when using the Internet

The Council respects an employee's right to a private life. However, the Council must also ensure that confidentiality about its business is maintained and that its employees and reputation are protected. It therefore requires that whenever an employee accesses a website, including for personal use, they ensure that they:

- Take care not to identify themselves as working for the Council where to do so may be a risk to their personal safety or be in any way detrimental to the carrying out of their duties. In particular on Social Media sites such as Facebook and Twitter.

- Do not conduct themselves in a manner that reveals personal, sensitive or confidential information held by the Council.

- Refrain from allowing their interaction on websites to damage working relationships between themselves and colleagues, clients or customers of the Council or bring the Council into disrepute. Examples of such interactions are set out at Appendix 4 and specifically cover:
  - Cyber-bullying
  - Expressing comments that can be clearly considered defamatory to another individual or group or which contravene an established council policy
  - Posting comments, videos or photos that reveal some form of personal work-related misbehaviour, for example about feigning illness or avoiding work

In addition to the above employees should not log into / stay logged into personal web sites during working time or spend time accessing the internet during working hours using their own smart phone or other personal equipment unless authorised to do so.

If any user is found to have breached this policy or evidence is revealed online of a breach of another Council policy, the Council's disciplinary procedure may be invoked. Further details regarding policy compliance are set out in Section 7.

6.4 Internet Account Management, Security and Monitoring

Access to the Internet is provided through your network login account and is monitored by the Council with all access recorded, logged and interrogated so that the Council:

- Can monitor total usage to ensure business use is not impacted by lack of capacity.
- Can plan and manage its resources effectively.
- Ensures that users act only in accordance with policies and procedures.
- Ensures that standards are maintained.
- Can prevent and detect any crime.
- Can investigate any unauthorised or inappropriate use.

Monitoring of access will only be undertaken by staff specifically authorised for that purpose.

Users must not break or attempt to break or circumvent any system security controls placed on their Internet Account.

Where a manager suspects that internet facilities are being abused by a user, they should inform their Director or Assistant Director who will, if they deem it appropriate, contact the Assistant Director (Corporate Services) to determine whether an investigation is appropriate.

As part of any authorised investigation, designated staff in CICT, Human Resources, Internal Audit, or Investigating Officers may investigate and access evidence from system audit logs, time recording systems etc.

In addition the Council will also comply with any legitimate requests from authorised bodies under the Regulation of Investigatory Powers legislation for information.

If any user is found to have breached this policy, they may be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed, further action may be taken to assist in the prosecution of the offender(s).

6.5 Things You Must Not Do

Access to the following categories of websites is currently blocked using a filtering system administered by CICT and the Council's Managed IT Services Provider.

- Illegal.
- Pornographic and/or other sexual explicit materials.
- Violence.
- Hate and discrimination.
- Offensive.
- Weapons.
- Hacking.
- Web chat.
- Gambling.
- Dating.
- Radio stations.
- Games.

Except where it is a necessary requirement for your work, you must **not** use your Internet account to:

- Create, download, upload, display or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene or offensive.
- Subscribe to, enter or use peer-to-peer networks or install software that allows sharing of music, video or image files.
- Subscribe to, enter or utilise real time chat facilities such as chat rooms, text messenger or pager programs (this does not include instant messaging for work purposes on Lync or Teams).
- Subscribe to, enter or use online gaming or betting sites.
- Subscribe to or enter "money making" sites or enter or use "money making" programs.
- Run a private business.
- For any illegal purpose e.g. buying and selling illegal or stolen goods etc. or committing, or attempting to commit fraud.
- To access materials of a violent or racist nature.
- To post information that harasses, intimidates, abuses, threatens or bullies others on any internet site.
- For any purpose which is inappropriate in the workplace by virtue of the fact that it may cause embarrassment or distress to another person or may bring the Council into disrepute.

- For accessing restricted sites or another users e-mail account without authorisation.
- For the transmission of confidential information outside the Council other than where it is done for “Whistle-blowing” purposes.
- For downloading and/or storing computer game programmes, music, videos or other files which could cause unacceptable congestion and disruption to the network and systems.
- For downloading and/or storing software without prior permission from the Council’s IT Managed Service provider.
- For intentionally accessing or transmitting information about, or software design for, breaching security controls or creating computer viruses.
- For downloading, copying or reposting copyrighted information or images without consent from the original source.
- For downloading any software that does not comply with the Council’s Policy.

The above list gives **examples** of “*unsuitable*” usage but is neither exclusive nor exhaustive. *“Unsuitable”* material would include data, images, audio files or video files the transmission of which is illegal under British law, and, material that is against the rules, essence and spirit of this and other Council policies.

Furthermore, the Councils information technology systems must not be used for any acts / purposes, even on behalf of elected Members of the Council where these would contravene the Prohibition of Political Publicity provisions of the Local Government Act 1986 (Appendix 2).

6.6 Your Responsibilities

It is your responsibility to:

- Familiarise yourself with the detail, essence and spirit of this policy before using the Internet facility provided for your work.
- Assess any risks associated with Internet usage and ensure that the Internet is the most appropriate mechanism to use.
- Know that you may only use the Council’s Internet facility within the terms of this policy.
- Read and abide by the terms of related policies set out in Section 10.

6.7 Line Manager’s Responsibilities

It is the responsibility of individual Line Managers to ensure that this policy is fairly and consistently applied and the use of the Internet facility is identified as being either:-

- Within an employees work time and relevant to and appropriate to the Council’s business and within the context of the users responsibilities.
- Within an employee’s own time and subject to the rules contained within this document.

It is the responsibility of individual Line Managers to guide staff and answer any questions about internet usage, by consulting with an Information Group representative if necessary.

Line managers must also monitor, report and deal with any inappropriate internet use by any member of their staff. Where a manager suspects that internet facilities are being abused by a user the guidance set out in Section 6.4 above should be followed.

6.8 Accidental Access to Restricted Sites

Should access be accidentally gained to an inappropriate site (such as those referred in Section 6.5 above) you must report this immediately to CICT. No action will be taken against employees who report such an event, as long as the inappropriate site is vacated as soon as is practicable and there is no pattern of inappropriate access.

6.9 Whom Should I Ask if I Have Any Questions?

This policy will be publicised and made available to all users on the Council's Intranet.

In addition all new Council Internet (and email) users must certify to say they have read, understood and accept the terms of use as set out in this policy (see Appendix 3). This should be forwarded to CICT so that internet user access can be set up.

Should employees have any questions regarding Internet use or about any aspects of the policy they should, in the first instance, refer them to their Line Manager. Information Governance group representatives and CICT staff may also be consulted for advice and assistance. Councillors should, in the first instance, refer any questions to Members' Service section.

Any queries of a technical nature about the Council's Internet service should be directed to CICT.

7 Policy Compliance

If any user is found to have breached this policy, they will be subject to the Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, you must seek advice from your Information Governance Representative or CICT.

8 Policy Governance

The following table identifies who within the Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Corporate Information Governance Group.
Accountable	Director of Resources and Development.
Consulted	Corporate Information Governance Group members, Trade Unions, Corporate Management Team.
Informed	All Councillors, council employees (including temporary staff) along with third parties, partners and contractual agents of the council as appropriate.

9 Review and Revision

This policy will be reviewed by the Council as it is deemed appropriate, but no less frequently than every 12 months.

10 References

The Council has a suite of Information Governance policy documents that are directly or indirectly relevant to this policy. These are:-

- Corporate Retention Policy
- Data Protection Policy
- Information Protection Policy
- Information Incident Management Policy
- Email Access Policy.
- IT Access Policy.
- Removable Media Policy
- Remote Working Policy.

Users should also be familiar with the following Council policy:-

- HBC Disciplinary Policy
- HBC Code of Conduct

In addition, there are a range of Human Resources related policies that are available on the council’s intranet.

It is the user’s responsibility to ensure their awareness of and compliance with all of these policies – further information can be obtained from Information Governance Group representatives or CICT.

11 Key Messages

- Users must familiarise themselves with the detail, essence and spirit of this policy before using the Internet facility provided. Use will be permitted only to staff that have been specifically designated as authorised users and have confirmed in writing that they accept and agree to abide by the terms of this policy.
- At the discretion of your line manager, and provided it does not interfere with your work, the Council permits a certain amount of personal use of its Internet facilities. This is limited to a maximum of 90 minutes per day) in your own time, outside of working hours (for example prior to work, during your lunch-break and following work) and is subject to the same standards as business use. The Council is not responsible for any personal transactions you enter into.
- Users are responsible for ensuring the security of their Internet account through appropriate use of a security logon-id and password.
- All internet access is recorded, logged and interrogated by the Council. Unauthorised or inappropriate use will be investigated
- Whenever an employee access a website, including for personal use, they should always conduct themselves in a way that guards their personal safety, does not damage working relationships and does not bring the Council into disrepute or contravene any of its policies.
- Users must ensure no personal, sensitive or confidential information held by the Council is revealed online.
- Employees should not spend time accessing the internet during working hours using their own smart phone or other personal equipment unless authorised to do so.

- Users must not create, download, upload, display or access knowingly sites that contain unsuitable material that might be deemed illegal, obscene or offensive or which contravenes the examples of unacceptable use set out in 6.5 of this policy.
- Line managers must deal with any inappropriate internet use by staff including by way of instructions and guidance through normal communication channels. However where a manager suspects that internet facilities have been or are being abused by a user, they should inform their Director or Assistant Director who will, if they deem it appropriate, contact the Assistant Director (Corporate Services) or the Head of Human Resources / Human Resources Manager to determine whether a detailed investigation is necessary.

Appendix 1 – Information Governance Group Representatives as at 16th Feb 2022

Information Governance Lead
Claire McLaren Tel 523003
Assistant Director (Corporate Services)

Data Protection Officer
Laura Stones Tel: 523087

Adults & Community Based Services Department
Trevor Smith Tel: 523950

Resources & Development Department / CICT *
Mike Smith Tel: 523758

Child & Joint Commissioning Department
Kay Forgie Tel: 284119

Neighbourhoods and Regulatory Services Department
Steve Russell Tel: 523031

In addition to the above the Council has specific roles identified which are also part of the overall approach to Information Governance arrangements and are involved in the Information Governance group:

Senior Information Risk Owner (SIRO)
Chris Little, Director of Resources and Development, Tel: 523003

Caldicott Guardian
John Lovatt, Assistant Director Adult Social Care Tel: 523903
For specific issues around social care (Advice and guidance on Caldicott matters should be request through Trevor Smith (Adults) or Kay Forgie (Children’s) on the telephone numbers above)

***** GENERAL CONTACT DETAILS
Contact with CICT Team on general issues should be made using 523764 or cict@hartlepool.gov.uk

Appendix 2 – Extract from the Local Government Act 1986

“Prohibition of political publicity

1. A local authority shall not publish any material which, in whole or in part, appears to be designed to affect public support for a political party.
2. In determining whether material falls within the prohibition regard shall be had to the content and style of the material, the time and other circumstances of publication and the likely effect on those to whom it is directed and, in particular, to the following matters:

   (a) Whether the material refers to a political party or to persons identified with a political party or promotes or opposes a point of view on a question of political controversy which is identifiable as the view of one political party and not of another;
   (b) Where the material is part of a campaign, the effect which the campaign appears to be designed to achieve.]

3. A local authority shall not give financial or other assistance to a person for the publication of material which the authority are prohibited by this section from publishing themselves”.

Appendix 3 – Internet & Email Form of Undertaking and Application Form

HARTLEPOOL
BOROUGH COUNCIL

Hartlepool Borough Council
Internet & E-mail Policy

Form of Undertaking

(I declare) I have read and understood the Hartlepool Borough Council Internet and E-mail policies and will abide by the instructions they contain and adhere to the principles expressed therein and those of the other Council Policies to which it refers.

Name: ………………………………………………………………………………

Department:……………………………………………………………………………

Phone / Ext No:……………………………………………………………………….

Payroll No:…………………………………………………………………………….

Signature:………………………………………………………………………………

Date:……………………………………………………………………………………

HARTLEPOOL
BOROUGH COUNCIL

Hartlepool Borough Council
Internet and E-mail Application Form

Name: ………………………………………………………………………………

Department:……………………………………………………………………………

Phone / Ext No:………………………………………………………………………..

Payroll No:……………………………………………………………………………….

Signature:………………………………………………………………………………

Date:………………………………………………………………………………………

Please tick box for service required

□ External E-mail facility

□ Internet access

Signed authorisation will be from the appropriate section head or their nominated representative.

Signature:……………………………. Date…………………………………

Completed copies should be sent to CICT, Civic Centre and also retained by Departments

Appendix 4 – Examples of Website Interaction that should be avoided

Employees should refrain from allowing their interaction on websites to damage working relationships between themselves and colleagues, clients or customers of the Council or bring the Council into disrepute. Examples of such interactions are set out at below.

Examples of Cyber-bullying
Cyber-bullying might include the following actions:

* Offensive posts – writing an offensive post about somebody on a blog, social networking or other website – even if this is meant as a joke – and continuing to do so having already been asked to stop. It may be that a person does not experience any direct form of cyber-bullying, being unaware that the bully is posting offensive messages about them on sites in the public domain.

* Threatening posts – this might also include ostensibly relatively inoffensive messages in terms of actual content but where it is the implied meaning behind the message that constitutes a form of bullying.

* Sharing a person’s private data online by posting personal details which they would not normally want to share with strangers or the general public, such as home address, phone numbers etc.

* Expressing comments that can be clearly considered defamatory to another individual or group

Examples of Other Inappropriate interaction
* Posting comments, videos or photos that reveal some form of personal work-related misbehaviour, for example about feigning illness or avoiding work.

* Making certain kinds of adverse or objectionable comments about the Council.

* Making comments that contravene Council policies, code of conduct or legislation in relation to acceptable behaviour. Examples may include comments in relation to political matters, those that contravene equality law etc.

The above is not intended to be an exhaustive list but provides examples and a guide to inappropriate online behaviour which could lead to the Council investigating and taking action under its disciplinary policy.

IMPORTANT
Employees should remember that everything shared on a website including a social networking site could potentially end up in the worldwide public domain and be seen or used by someone you did not intend, even if it appears to be ‘private’ or is on a closed profile or group.