HARTLEPOOL
BOROUGH COUNCIL

Policy Document

Email Policy
v6.0

May 2022

Document Control

Organisation	Hartlepool Borough Council
Title	Email Access Policy
Author	Paul Diaz
Date created	September 2011
Next review date	May 2023

Revision History

Revision Date	Reviser	Version	Description of Revision
Nov 10	Alison Oxley	1	
Sept 11	Paul Diaz	2	
March 15	Kay Forgie	3	
Feb 17	S Russell	3.1	Minor format changes
May 18	P Diaz	3.2	Updates for GDPR
Feb 19	P Diaz	3.3	Updates due to GCSX retirement
Feb 2020	Kay Forgie	4.0	Updates to secure email and internal use only emails
May 2021	Kay Forgie	5.0	Reference to software policy removed. Notification of virus amended to include email abuse address.
May 2022	Mike Smith	6.0	Phishing email referenced Minor wording changes for clarification

Document Approvals

Version	Approved by	Date approved
3.1	Information Governance Group	17 February 2017
3.2	Information Governance Group	May 2018
3.3	C Little, Director of Finance & Policy (SIRO)	26th March 2019
4.0	C Little, Director of Finance & Policy (SIRO)	20th July 2020
5.0	C Little, Director or Resources and Development (SIRO)	7th June 2021
6.0	C Little, Director of Resources and Development (SIRO)	19th May 2022

1 Policy Statement

Hartlepool Borough Council will ensure all users of Council email facilities are aware of the acceptable use of such facilities.

2 Purpose

The objective of this Policy is to direct all users of Council email facilities by:

- Providing guidance on expected working practice.
- Highlighting issues affecting the use of email.
- Informing users about the acceptable use of ICT facilities in relation to emails.
- Describing the standards that users must maintain.
- Stating the actions that may be taken to monitor the effectiveness of this policy.
- Warning users about the consequences of inappropriate use of the email service.

The Policy establishes a framework within which users of Council email facilities can apply self-regulation to their use of email as a communication and recording tool.

3 Scope

This policy covers all email systems and facilities that are provided by Hartlepool Borough Council for the purpose of conducting and supporting official business activity through the Councils network infrastructure and all stand alone and portable devices.

This policy is intended for all Hartlepool Borough Council Councillors, Committees, Departments, Partners, Employees of the Council, contractual third parties and agents of the Council who have been designated as authorised users of email facilities.

The use of email facilities will be permitted only by staff that have been specifically designated as authorised users for that purpose, and have confirmed in writing that they accept and agree to abide by the terms of this policy.

The policy also applies where appropriate to the internal Microsoft exchange e-mail facility.

The use of email facilities by staff that have not been authorised for that purpose will be regarded as a disciplinary offence.

4 Definition

All email prepared and sent from Hartlepool Borough Council email addresses or mailboxes, and any non-work email sent using Hartlepool Borough Council ICT facilities is subject to this policy.

5 Risks

Hartlepool Borough Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Failure to report information security incidents
- Inadequate destruction of data
- Loss of direct control of user access to information systems

- Exposure to legal action and / or adverse publicity
- Time wasting by inappropriate and unauthorised use
- Incorrect handling of CONFIDENTIAL information see below

If there any questions or doubts about which category the information you are dealing with falls into then you should contact your Departmental Information Governance representative (see Appendix 1 for details).

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

6 Applying the Policy

6.1 Email as Records

All emails that are used to conduct or support official Hartlepool Borough Council business must be sent using a "@hartlepool.gov.uk" address. Any exceptions to this must be agreed by the corporate IG group.

Staff **must not** use non-work email accounts to conduct or support official Hartlepool Borough Council business. Councillors, using secure non hartlepool.gov.uk accounts must ensure that any emails containing sensitive or confidential information are sent securely and clearly marked as CONFIDENTIAL. A list of secure domains is available on the HBC Intranet (http://hbcintranet/ICT_Support/Pages/Secure-Email-Domains.aspx). If the external email domain is not on the list then it must be sent via approved encrypted means. Contact your departmental IG representative for more information. All emails that represent aspects of Council business or Council administrative arrangements are the property of the Council and not of any individual employee.

Users should be aware any emails and attachments may need to be disclosed under the Regulation of Investigatory Powers Act (RIPA), The Data Protection Act 2018, UK General Data Protection Regulations (GDPR), subject access request provisions or the Freedom of Information Act.

Emails held on Council equipment are considered to be part of the corporate record and email also provides a record of staff activities. Email accounts will be deleted 1 month after users have left the Authority. Managers may request accounts are kept for longer if required for business purposes. An end date must be specified.

The legal status of an email message is similar to any other form of written communication. Consequently, any e-mail message sent from a facility provided to conduct or support official Hartlepool Borough Council business should be considered to be an official communication from the Council. In order to ensure that Hartlepool Borough Council is protected adequately from misuse of e-mail, the following controls will be exercised:

i. It is a condition of acceptance of this policy that users comply with the instructions given during the Email and Information Governance training sessions and e-learning courses.

ii. All official external e-mail must carry the following disclaimer:

*"*This document is strictly confidential and is intended only for use by the addressee. If you are not the intended recipient, any disclosure, copying, distribution or other action taken in reliance of the information contained in this email is strictly prohibited.

Any views expressed by the sender of this message are not necessarily those of Hartlepool Borough Council. If you have received this transmission in error, please use the reply function to tell us and then permanently delete what you have received.

Please note: Incoming and outgoing e-mail messages are routinely monitored for compliance with our policy on the use of electronic communications."

iii. Signatures must follow the corporate standard (these are added in Outlook - contact CICT for assistance) and contain the following details:-

Name | Post Title
Hartlepool Borough Council
Tel: (01429 xxxxxx

Email: xxxx.xxxx@hartlepool.gov.uk
Web: hartlepool.gov.uk
Facebook: facebook.com/hartlepoolcouncil
Twitter: twitter.com/HpoolCouncil

The Councils website and social media addresses are added automatically in the footer of any external hartlepool.gov.uk email.

Whilst respecting the privacy of authorised users, Hartlepool Borough Council maintains its legal right, in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA), to monitor and audit the use of email by authorised users to ensure adherence to this Policy. Any such interception or monitoring will be carried out in accordance with the provisions of that Act. Users should be aware that deletion of e-mail from individual accounts does not necessarily result in permanent deletion from the Council's ICT systems.

It should also be noted that email and attachments may need to be disclosed under the RIPA, Data Protection Act 2018, UK GDPR or the Freedom of Information Act 2000. Further information regarding this can be obtained from Corporate ICT (CICT) team.

6.2 Email as a Form of Communication

Email is designed to be an open and transparent method of communicating. However, it cannot be guaranteed that the message will be received or read, nor that the content will be understood in the way that the sender of the email intended. It is therefore the responsibility of the person sending an email to decide whether email is the most appropriate method for conveying time critical or confidential information or of communicating in the particular circumstances.

All emails sent to conduct or support official Hartlepool Borough Council business must comply with corporate communications standards. Hartlepool Borough Council's Communications Policy must be applied to email communications.

Email must not be considered to be any less formal than memos or letters that are sent out from a particular service or the authority. When sending external email, care should be taken not to contain any material which would reflect poorly on the Council's reputation or its relationship with customers, clients or business partners.

Under no circumstances should users communicate material (either internally or externally), which is, for example, defamatory, obscene, or does not comply with the Council's Equal Opportunities Policy, or which could reasonably be anticipated to be considered inappropriate. Any user who is unclear about the appropriateness of any

material, should consult their line manager prior to commencing any associated activity or process.

IT facilities provided by the Council for email should not be used:

- For the transmission of unsolicited commercial or advertising material, chain letters, or other junk-mail of any kind, to other organisations.
- For the unauthorised transmission to a third party of CONFIDENTIAL material concerning the activities of the Council.
- For the transmission of material such that this infringes the copyright of another person, including intellectual property rights.
- For activities that unreasonably waste staff effort or use networked resources, or activities that unreasonably serve to deny the service to other users.
- For activities that corrupt or destroy other users' data.
- For activities that disrupt the work of other users.
- For the creation or transmission of any offensive, obscene or indecent images, data, or other material, or any data capable of being resolved into obscene or indecent images or material.
- For the creation or transmission of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- For the creation or transmission of material that is abusive or threatening to others, or serves to harass or bully others.
- For the creation or transmission of material that either discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs.
- For the creation or transmission of defamatory material.
- For the creation or transmission of material that includes false claims of a deceptive nature.
- For so-called 'flaming' - i.e. the use of impolite terms or language, including offensive or condescending terms.
- For activities that violate the privacy of other users.
- For unfairly criticising individuals, including copy distribution to other individuals.
- For disclosing to others any information given in document classified with a protective marking without the prior consent of a person authorised to give it, unless under a requirement of law.
- For the creation or transmission of anonymous messages - i.e. without clear identification of the sender.
- For the creation or transmission of material which brings the Council into disrepute.
- Printing off large volumes of personal emails and/or attachments using work printers unless arrangements have been made to reimburse the cost to the Council.
- Reading lengthy incoming personal emails and/or attachments during working hours.
- Drafting and/or sending an unreasonable amount of outgoing personal emails during working hours.
- Registering for websites that are not connected to Council business

6.3 Acceptable use of the Council's e-mail facility and addresses includes

- Receiving small numbers of personal emails
- Printing off the occasional personal email and/or attachment using work printers
- Opening and identifying an email as being personal (once recognised as being personal the remainder of the email should not be read during working hours unless it is very short)
- Reading lengthy incoming personal emails and/or attachments outside of working hours

- Drafting and/or sending outgoing personal emails and/or attachments outside of working hours

Whilst employees have no control over incoming personal emails, they are responsible for ensuring these do not adversely impact on the Council's email facility (in terms of quantity and size of attachments or by 'clogging up' individual mail boxes). Personal emails using Council facilities are subject to the same conditions as business use. Further guidance on what is acceptable and unacceptable use (for example what might constitute large volumes of personal email / lengthy incoming personal emails) is available from Workforce Services.

6.4 Junk Mail

There may be instances where a user will receive unsolicited mass junk email or spam. It is advised that users delete such messages without reading them. Do not reply to the email. Even to attempt to remove the email address from the distribution list can confirm the existence of an address following a speculative e-mail.

Before giving your e-mail address to a third party, for instance a website, consider carefully the possible consequences of that address being passed (possibly sold on) to an unknown third party, and whether the benefits outweigh the potential problems.

Chain letter e-mails (those that request you forward the message to one or more additional recipients who are unknown to the original sender) **must not** be forwarded using Hartlepool Borough Council systems or facilities.

6.5 Mail Box Size

In order to ensure that the systems enabling email are available and perform to their optimum, users should endeavour to avoid sending unnecessary messages. In particular, the use of the "global list" of e-mail addresses is discouraged.

Users are provided with a limited mail box size to reduce problems associated with server capacity. Email users should manage their email accounts to remain within the limit, ensuring that items are filed or deleted as appropriate to avoid any deterioration in systems.

Email messages can be used to carry other files or messages either embedded in the message or attached to the message. If it is necessary to provide a file to another person, then a reference to where the file exists should be sent rather than a copy of the file. This is to avoid excessive use of the system and avoids filling to capacity another person's mailbox. If a copy of a file must be sent then it should not exceed 10 mb in size.

6.6 Monitoring of Email Usage

All users should be aware that email usage is monitored and recorded centrally. The monitoring of email (outgoing and incoming) traffic will be undertaken so that Hartlepool Borough Council:

- 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 use.

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

These arrangements will be applied to all users and may include checking the contents of email messages for the purpose of:

- Establishing the existence of facts relevant to the business, client, supplier and related matters.
- Ascertaining or demonstrating standards which ought to be achieved by those using the facilities.
- Preventing or detecting crime.
- Investigating or detecting unauthorised use of email facilities.
- Ensuring effective operation of email facilities.
- Determining if communications are relevant to the business.

Where a manager suspects that the email 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).

As part of any authorised investigation, designated staff in CICT, Human Resources or Internal Audit 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 Hartlepool Borough 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).

6.7 Categorisation of Messages

When creating an email, the information contained within it must be assessed and classified by the owner according to the content, when appropriate.

6.8 Security

Emails sent between @hartlepool.gov.uk addresses are held with the same network and are deemed to be secure. However, emails that are sent outside this closed network travel over the public communications network and are liable to interception or loss. There is a risk that copies of the email are left within the public communications system. Therefore, CONFIDENTIAL material must not be sent via email outside this closed network, unless it is being sent to another secure domain as listed in the secure domain list on the HBC Intranet.

Where the sender and receiver domains of the email message are on the secure domain list then this **can be used** for communicating CONFIDENTIAL material externally.

6.9 Confidentiality

All staff are under a general requirement to maintain the confidentiality of information. There are also particular responsibilities under Data Protection legislation to maintain the confidentiality of personal data. If any member of staff is unsure of whether they should pass on information, they should consult their Departmental Information Governance Representative or CICT.

Staff must make every effort to ensure that the confidentiality of email is appropriately maintained. Staff should be aware that a message is not deleted from the system until all recipients of the message and of any forwarded or attached copies have deleted their copies. Moreover, confidentiality cannot be assured when messages are sent over outside networks, such as the Internet, because of the insecure nature of most such

networks and the number of people to whom the messages can be freely circulated without the knowledge of Hartlepool Borough Council.

Care should be taken when addressing all emails, but particularly where they include CONFIDENTIAL information, to prevent accidental transmission to unintended recipients. Particular care should be taken if the email client software auto-completes an email address as the user begins typing a name. This function has been disabled on all HBC email accounts.

All external email addresses that are included in the council's Outlook address book must be marked as EXTERNAL. If an employee identifies an incorrect email address in the Outlook address book this must be reported to CICT.

Automatic forwarding of email (for example when the intended recipient is on leave) must be considered carefully to prevent CONFIDENTIAL material being forwarded inappropriately. Rules can be implemented to include or exclude certain mail based on the sender or subject. If you require automatic forwarding, please contact your IG representative who will request approval from the corporate IG group.

The automatic forwarding of email to a non-secure email domain (i.e. one not listed on the HBC secure domain list) contradicts national guidelines and is therefore not acceptable.

6.10 Negligent Virus Transmission

Computer viruses are easily transmitted via email and internet downloads. Full use must therefore be made of Hartlepool Borough Council's anti-virus software. If any user has concerns about possible virus transmission, they must report the concern to CICT

In particular, users:

- Must not transmit by email any file attachments which they know to be infected with a virus.
- Must not download data or programs of any nature from unknown sources.
- Must ensure that an effective anti-virus system is operating on any computer which they use to access Council facilities.
- Must not forward virus warnings other than to email.abuse@hartlepool.gov.uk and CICT
- Must report any suspected files to CICT
- Must not click on any links in unexpected emails. If this is done accidentally, you must contact CICT by phone or in person immediately.

In addition, the Council will ensure that email is virus checked at the network boundary and at the host, and where appropriate will use two functionally independent virus checkers.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing the virus to be transmitted.

6.11 Accessing Emails using Outlook Web Access

Currently in order to access HBC Outlook accounts remotely the following actions are necessary (whether it be on a computer or Smartphone):

1. Link to https://autodiscover.hartlepool.gov.uk/owa enter hbc\yourusername and password

2. Read emails – Councillors and Users must not open attachments which may contain sensitive or confidential information as this can result in a temporary copy being stored on the device.

All users **must not** use applications to store passwords as this effectively means that the only security in place on Smartphones to prevent unauthorised access to HBC email is a pin on the phone (provided one has been set up) which any mobile phone shop will unlock on request. For clarity this means if your phone is stolen, misplaced etc then once unlocked anyone would potentially have access to your email account and everything it contains.

All staff are therefore instructed that anyone accessing council emails on personal Smartphones do not do so via one of these apps, but instead ensure they use the browser and input their username and password each time.

6.12 Phishing Emails

Users must be aware of the dangers of “Phishing” emails. These emails are designed to lure recipients into providing sensitive data such as passwords, banking and credit card details or other personally identifiable information. This information is then used to breach network security to steal data or introduce viruses or ransomware, access bank details or commit identity theft.

To successfully "phish" personal information, the message must get the user to go to a website. Phishing messages will almost always tell them to click a link that takes them to a site where their personal information is requested. Legitimate organisations would never request this information via email or instant messages.

Therefore, users are reminded to be wary of emails asking them to login to any system to view/download files, consider:

- Were you expecting this email or has it come expectantly even if it is from a known sender?
- Has the user ever previously asked you to login to a system to view/download files?
- Are you able to verify with the sender by phone or in person that the email is genuine?
- A standard tactic is to try to force users to respond quickly to reduce the chance of thinking too much. Typically they are to made to feel that they need to hurry because the email is from someone important or their account will be suspended if they do not respond by a deadline.

6.13 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 email (and internet) users must certify to say they have read, understood and accept the terms of use as set out in this policy (see Appendix 2). 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 refer any questions, in the first instance, to the Members’ Services section.

Any queries of a technical nature about the Council’s Internet and Email services should be directed to CICT.

7 Policy Compliance

If any user is found to have breached this policy, they may be subject to Hartlepool Borough 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).

Email is a business tool and as such can be audited and inspected without notice to users.

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

8 Policy Governance

The following table identifies who within Hartlepool Borough 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

Hartlepool Borough 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
- Internet Acceptable Use Policy
- IT Access Policy.
- Removable Media Policy
- Remote Working Policy.

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

- HBC Disciplinary Policy

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

- All emails sent by staff that are used to conduct or support official Hartlepool Borough Council business must be sent using a "@hartlepool.gov.uk" address.
- All emails containing CONFIDENTIAL information sent from a HBC account must be sent to an equally secure recipient domain as listed in the secure domain list, or via an alternative approved encrypted means.
- Non-work email accounts **must not** be used to conduct or support official Hartlepool Borough Council business.
- Work email cannot be used for registering for websites that are not connected to Council business
- Staff must ensure that any emails containing sensitive information are sent securely from an official council email account.
- All official external e-mail must carry the official Council disclaimer (see section 6.1).
- Under no circumstances should users communicate material (either internally or externally), which is defamatory, obscene, or does not comply with the Council's Equal Opportunities policy.
- Where both email domains are listed on the secure domain list (i.e. the sender and receiver domains), this **must be used** for communicating CONFIDENTIAL material externally.
- Automatic forwarding of email must be considered carefully to prevent material being forwarded inappropriately. Approval must be sought from CICT.

Appendix 1 – Information Governance Group Representatives as at 7th June 2021

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 number above)

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

Appendix 2 – Internet & Email Form of Undertaking and Application Form

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
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 within Departments by the appropriate section head or nominated representative countersigning above.