The Highland Council
Comhairle na Gàidhealtachd

ICT Acceptable Use Policy (AUP)

Version Control

Version	Revision	Date	Author (s)	Distributed	Notes
1.2	Issued	02/02/2000			
1.3	Issued	05/02/2010	Judy Wyld/Jon Shepherd/Vicki Nairn	Resources Committee Trade Unions Personnel Internal Audit Legal Services	
2.0	Issued	11/3/2010	Judy Wyld/Jon Shepherd/Vicki Nairn	Resources Committee Trade Unions Personnel Internal Audit Legal Services	Current Live version
3.0	Issued	25/01/2011	Linda Johnstone/John Grieve	Updated on intranet	Sections 2. Amalgamate 2 sentences into 1 with no change to scope of the policy merely easier to read for end user 3.5. Unblock website governance process update to reflect current practice 4. link removed as site is no longer existent
4.0	Issued	29/06/2012	John Grieve/Dave Barker	Updated on intranet	Additional new section (3.12) highlighting potential monitoring of email sent via GSX as a result from the RAP
5.0	Issued	21/05/2013	Philip Mallard, Senior Information & Security Officer	Finance, Housing & Resources Committee	Review of AUP. 1) Renamed document to align with name that is generally used to refer to the policy 2) Scope of policy clarified and new references to specific education use of ICT. 3) Document restructured 4) Improvements to provide a clearer policy statement on monitoring and investigations. (Responding to internal audit recommendations).
5.1	Issued	25/02/2015	Philip Mallard, Senior Information & Security Officer	Resources Committee	Annual Review. Addition of text to reflect changes to routine monitoring of staff internet usage. Minor changes to description of process to better reflect its scope and purpose. Approved at Resources Committee

1 Purpose of the policy

The purpose of this policy is to ensure that all users of the Highland Council's Information and Communications Technology (ICT) are clear about what is acceptable and unacceptable ICT usage. It also sets out the monitoring of user activity that takes place, how the Highland Council will use this, and the rights of access the council has to information held on its systems.

2 Scope of the policy

This policy applies to **all** Highland Council employees, agents of the Council, persons representing the Council (including sub-contractors and consultants), Trade Union representatives, Elected Members, and school pupils.

In order to ensure this overarching AUP is relevant in an education context simplified versions have been made available for pupils of different ages to promote understanding of the behaviours that are expected of them, as well as acceptable / unacceptable use. These simplified pupil AUPs are an interpretation of this Policy, and do not replace it. In particular, the approach to Council monitoring is fully covered in this Policy. It is the responsibility of Head Teachers and Teachers to ensure that all pupils within their school are aware of their responsibilities. Teachers and other school staff are fully covered by this ICT AUP, as with other members of staff.

The term ICT covers all computing devices (including mobile devices), telephones (including mobile phones), printers and photocopying devices (including multifunctional devices). It also refers to Information Systems, all software, networks, internet access and email systems.

This policy applies to all aspects of ICT use, whether undertaken in a Council location or elsewhere, including the use of any separate standalone systems which are provided by the council (or its ICT providers), or used to conduct business on behalf of the Highland Council. If, in any circumstances, privately owned ICT facilities are used when any of the above identified groups undertake business on behalf of The Highland Council, then their usage must conform to this policy.

The policy statements regarding monitoring of ICT relate to the technical measures that are in place to monitor activity on council ICT and therefore apply to all users of Council provided ICT (either direct or through ICT providers contracted by the Council).

3 Policy revisions and user communication

Version control changes are recorded in the table at the front of the document. The most current copy of the policy is available on the Highland Council's intranet and website.

4 ICT Acceptable Use Policy Statement

4.1 Expectation of proper conduct

The effective operation of the Council's ICT systems relies heavily on the proper conduct of the users. The use of all ICT facilities must be in compliance with all appropriate legislation, relevant codes of conduct and the Highland Council Policies.

In particular, those in scope of this policy must only use ICT that has been authorised for their use. Any attempt to gain unauthorised access to any system provided by the council or use the Council ICT to gain unauthorised access to any other system may be a breach of this policy, and may also be a breach of legislation (including the Computer Misuse Act 1990).

By using any Council ICT the user agrees to use it in accordance with this policy as a condition of being provided with access to it.

4.2 Consequences of Misuse

The Highland Council may at its sole discretion, suspend or terminate ICT access, withdraw or remove any material uploaded by the user in contravention of this Policy. The Highland Council may take such action as it considers necessary, including taking disciplinary action or disclosing information to law enforcement agencies.

Pupils who are deemed to have breached this policy may be subject to the disciplinary procedures within their school and appropriate sanctions may be applied.

Any other ICT users that are not employed by The Highland Council and not subject to the council disciplinary procedure will be subject to provisions in the contract held with them or other acceptable use agreement they have entered into.

In any event misuse may result in the withdrawal of ICT, legal action or involvement of law enforcement agencies. ICT users should be aware that use of Council ICT is monitored at all times and monitoring information is retained and used for both routine monitoring reports and to support potential misuse reports.

4.3 Acceptable Use

The following criteria will be used where relevant to assess whether usage is acceptable:

- be in support of business and service needs consistent with the Highland Council policies;
- be in support of an individual's approved duties/remit;
- be consistent with the Council policy, procedure and guidance that is appropriate to any system or network being used / accessed;
- be consistent with appropriate provision of education;
- the handling of the information is appropriate for the type of information;

- is limited personal use as defined in 4.4 Personal Use of Council ICT;
- any use of social media is consistent with the Policy on the Acceptable Use of Social Media**;**
- any reasonable activity undertaken by authorised ICT security personnel as part of approved duties / remit, including gathering information as part of specific potential misuse reporting or undertaking ICT Security Threat Monitoring (section 5.3).

4.4 Personal Use of Council ICT

ICT equipment and services may be used for limited personal usage provided that:

- this is not associated with monetary reward;
- is undertaken in the user's own time (non-work hours e.g. break times, before or after work);
- is not interfering with the delivery of Council services;
- does not violate this or any other Council policies and is a lawful activity.

Any questions or guidance about acceptable usage should be discussed with the individual's supervisor (or teacher for pupils).

4.5 Security

All Users must:

- not share their account passwords or allow another person to use their account(s);
- not use or attempt to use another individual's account;
- not leave unattended ICT equipment logged on without first locking the device (if a lock facility is not available then the user must log out.);
- notify the Service Desk and their line manager if they suspect or identify a security problem or a breach of the ICT Acceptable Use Policy by any user;
- take reasonable precautions to protect the Council's ICT from security issues such as computer viruses and malware. To reduce the risk of potential viruses and malware, users should not open any suspicious email attachments or independently load any software, including screensavers, onto their computers. If a user does inadvertently open a message or attachment that contains a virus or malware, they should contact the Service Desk immediately;
- use only properly supplied and authorised systems for undertaking Council business;
- where enabled, make use the Council's protective marking technology in accordance with provided guidance and take full account of the notices provided;
- use only the authorised software to access the internet.

School Pupils do not have direct access to the Service Desk and must therefore notify their teacher if they identify any security issue. The teacher is then responsible for reporting this to the Service Desk.

4.6 Unacceptable Use

It is unacceptable for a user to use, submit, publish, display, download or transmit on or from the network or on any Council ICT system or device which connects to the Council network or is operated by the Council (or our ICT providers) any information which:

- restricts or inhibits other users from using the system or impairs the efficiency of the ICT systems;
- violates or infringes upon the rights of any other person, including the right to privacy;
- Is contrary to the Council's Harassment at Work and Grievance and Harassment Policies (or equivalent school policies);
- contains defamatory, abusive, obscene, pornographic, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- encourages the use of controlled substances or uses the system with criminal intent;
- uses the system for any other illegal purpose;
- breaches legislation or statutory requirements which the Council has to comply with e.g. Data Protection Act 1998, Copyright Designs & Patents Act 1988.

It is unacceptable for a user to use the facilities and capabilities of the ICT systems to:

- conduct any non-approved business;
- download or install any unauthorised software;
- undertake any activities detrimental to the reputation of the Highland Council;
- transmit material, information, or software in violation of any local, national or international law;
- undertake, plan or encourage any illegal purpose;
- deliberately contribute to websites that advocate illegal activity;
- harass an individual or group of individuals;
- make offensive or derogatory remarks about anybody on social media and discussion forums;
- post offensive, obscene or derogatory content (including photographs, images, commentary, videos or audio) on social media and discussion forums;
- create or share any content which breaches confidentiality;
- view, transmit, copy, download or produce material, including (but not exhaustively) software, films, television programmes, music, electronic documents and books which infringes the copyright of another person, or organisation;
- conduct any unauthorised political activity;
- conduct any non-Highland Council approved fund raising or non-Highland Council related public relations activities;
- access or transmit information via the Internet, including email, in an attempt to impersonate another individual;
- attempt to gain deliberate access to facilities or services which you are unauthorised to access;
- attempt to bypass the Highland Council internet filtering or any ICT monitoring functions;
- attempt to bypass the Council's protective marking technology or select (or downgrade to) an inappropriate security classification for an email or document for the purposes of bypassing the security controls;

- deliberately undertake activities that corrupt or destroy other users' data; disrupt the work of other users, or deny network resources to them; violate the privacy of other users;
- send sensitive personal data by email to unsecure external email addresses/contacts (unless a secure method is used, or the customer has requested the data to be sent to them and a risk assessment has identified this as being appropriate).

Only hardware and software that has been authorised for use by ICT Services are acceptable for Internet and Email access use.

The previous items are examples of unacceptable use but this is not an exhaustive list and each potential breach of ICT AUP would be assessed on its individual circumstances. If a user is in any doubt about what constitutes acceptable or unacceptable use they should seek clarification from their line manager (or teacher for pupils).

4.7 Filtering and inadvertent access to inappropriate material

Access to the Internet via The Highland Council's systems is "filtered". The intention is to prevent access to certain sites that could be inappropriate or damaging to council systems, for example, those containing pornography or malware. The system, however, is not fail-safe and the Highland Council cannot prevent the possibility that some sites are accessible e.g. newly added sites which have not been detected by our systems to be blocked that are inconsistent with the policies of the Council, or not in line with the employee's normal duties and responsibilities.

Where material which is not consistent with the policies of the Council (including this Acceptable Use Policy) is inadvertently accessed, users must report the matter to their line manager and to the Service Desk immediately (or to a teacher for pupils). If there is any doubt as to what constitutes inappropriate material, the user should seek advice from their line manager (or teacher for pupils) or ICT Services. If a user continues to access inappropriate material this will be treated as unacceptable usage as outlined within this policy.

4.8 Use of Email

The internal email service is secure and can be used for communicating confidential and personal data, but any email communication and sharing of information by email must be appropriate (that is it must be appropriate for all recipients of an email to see the information contained within the body and any attachments of the email).

Externally addressed email is often not secure. Any material that is sensitive personal data, confidential or valuable to the Council should not be emailed externally unless encrypted or sent through a secure service. For communication with some government agencies secure email is available through the normal Council email system.. If you are in any doubt about the security of email then you must seek advice from your line manager before sending the email.

If a member of the public requests their personal data to be emailed to them, then this can be done if they are fully understand of the risk and confirm that they want to accept that risk. If this involves sensitive personal data then this permission must be in writing and retained as a Council Record. Even with this consent from the subject, it is important to ensure that personal data of a third party is not included and that risks have been considered. If there is any doubt then the email should not be sent.

E-mail can result in binding contracts. Users should be aware that legal commitments can result from their emails, and the same degree of care should be exercised as with any other written communication.

4.9 Dissemination of information

When disseminating views or opinions via Council systems, on subjects not directly related to their responsibilities in the Council, users must ensure that any opinions or views expressed are not attributed to the Council by inserting the following phrase:

“The opinions expressed herein are my own and do not necessarily reflect those of the The Highland Council”

The use of this disclaimer does not allow users to undertake any activity which is otherwise contrary to this Policy.

5 Monitoring usage of ICT and user activity

5.1 Overview of Council monitoring

Misuse of ICT facilities can have a negative impact upon employee productivity, the performance of the network, the security of the network, our ICT Infrastructure and the reputation of the Council.

The Highland Council's ICT equipment and resources are provided for the purpose of undertaking Council business (including education). Therefore, the Council maintains the right to examine any systems, inspect any data recorded in those systems, and disclose information to support Council business or as legally required. Users should be aware that emails content, email usage, detailed internet usage, telephony usage and ICT usage is recorded and retained by the Council.

The volume of internet and network traffic, together with the internet sites visited, and the volume and types of any files downloaded are routinely monitored and recorded. This is done for the purposes of ICT performance and security monitoring and to identify any unusual or unacceptable user activity that could be a breach of this ICT AUP. The specific content of any transactions undertaken via a permitted website will not be monitored unless there is a suspicion of improper use.

The Council uses monitoring and filtering tools that will block access to some websites. If a user attempts to visit a web page that is blocked then a message indicating that access is restricted will be displayed in the browser. Any attempt to circumvent such restrictions will constitute a breach of the ICT AUP. If access to a blocked site be required for business reasons then this may be requested, and any such request will be subject to an ICT governance process. ICT Users should be aware that when web pages are blocked that this results in automated alerts being generated that identify the ICT users and the reason for the block. These alerts are evaluated by security personnel (both within the Council and our ICT providers) and follow up action may be taken in accordance with this Policy.

In order to ensure compliance with this policy, the Council also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and can check for the use of any rude or offensive words or phrases.

The Council will use protective marking technology to support users with marking the security classification of their emails and documents. Users should be aware that this system records monitoring information on their activities such as the choice of security classification and any justifications for proceeding when warned about an action. This information may be accessed as part of routine reporting to identify pattern, improve configuration of the software and to improve staff guidance. It may also be used as part of potential misuse reporting, following the approval process, as set out in section 6.

If there is reason to suspect that there has been improper use of ICT by a specified ICT user, further targeted monitoring may be undertaken with or without the individual’s knowledge, subject to the appropriate approval being gained as set out in section 6 of this policy.

5.2 Routine Monitoring reports

Reports on ICT usage (including internet and email) will be provided to nominated managers that identify individual user activity (such as volume of internet usage), or storage for file types that could indicate breaches of copyright. Managers and users should be aware that high internet usage does not in itself constitute a breach of the ICT AUP, but if there is no business reason for this it could justify further investigation.

If the nominated manager requests further details based on these reports, then a more detailed user report will be provided. No further information will be provided without following the Potential Misuse Reporting approval process.

If any routine monitoring identifies user activity that could constitute a breach of the ICT AUP then this will be logged as a security incident by ICT Services and follow-up action taken.

5.3 ICT Security Threat Monitoring

The Council uses a range of technology to proactively monitor threats to its network and infrastructure. Where this monitoring identifies a potentially immediate or high risk threat to the security of the Council's network or infrastructure, with the permission of the Head of Digital Transformation or ICT Operations Manager, monitoring information shall be used by security personnel (within the Council and its ICT providers) to identify more information on the threat and to enable a prompt response to be made. Where necessary to understand the threat, this will require access to be made to detailed monitoring information. Access to this monitoring information shall be on a need to know basis, with minimum detail being accessed, as required to deal with the immediate security threat.

A security incident shall be logged for each incident that is investigated and where monitoring information has been accessed that includes identifiable user activity this will be recorded as part of this incident. The information gained through this activity shall not be used for any other purpose other than specified below.

If this activity identifies potential misuse by a specific ICT user then a follow-up action will be to instigate the approval process to create a potential misuse report (in accordance with section 6 of this Policy).

5.4 GCSx Interception & Monitoring

Users who have been set up with access to the Public Services Network (PSN) and the Government Connect Secure Extranet (GCSx) email facility should be aware that emails can be intercepted, monitored and/or recorded for legal purposes by Government Communication Head Quarters (GCHQ).

5.5 Other external interception & monitoring

Users should be aware that any email that leaves Council systems (i.e. external email) and internet usage is be monitored by external bodies such as internet service providers (ISP). The Council's internet service is monitored by our ISPs.

6 Information Security Incidents and Potential Misuse Reporting

6.1 Information Security Incident Management Procedure

Potential breaches of the ICT AUP will be reviewed by authorised security personnel from ICT Services following the Information Security Incident Management Procedure.

ICT Services follows an operational procedure for the management of Information Security incidents. This includes potential breaches of the ICT AUP as well as security concerns that may not be related to user misuse e.g. malware. It ensures a consistent approach is taken when reviewing each security incident. Changes to this operational procedure will be agreed by the Head of Digital Transformation.

6.2 Information Security incident identification and logging

Any user can raise an information security incident by calling the Service Desk. Staff are required to do this where they identify any information security concern or potential breach of the ICT AUP.

All information security incidents raised through the Service Desk will be evaluated by ICT Services security personnel but not all information security incidents will result in a potential misuse report being produced. This will be dependent on the severity of the security incident and the circumstances. ICT Services will keep records of all reported security incidents.

6.3 Evaluation of security incidents

The ICT AUP sets out what is considered to be acceptable and unacceptable and this policy statement will be used by ICT Services to identify if the information security incident is a potential breach of the ICT AUP.

ICT Services will use the information provided as part of the logging of the security incident to assess whether there is a potential breach of the ICT AUP. If there is insufficient information then the ICT users involved may be contacted by ICT Services to identify further information and full cooperation must be provided by users. At this stage detailed user specific monitoring information will not be accessed.

If the circumstances make contact with the users involved difficult or inappropriate, then the process may be started for a Potential Misuse Report to be created in order to enable access to detailed user specific monitoring information.

If the incident may involve a breach of the Data Protection Act 1998, then the relevant Information Asset Owner (of the information involved in the breach) will be required to complete a Data Protection Breach Report. If there is suspicion of specific user misuse relating to this Data Protection breach, then this may also require the process to be started for a Potential Misuse Report to be created.

6.4 Potential Misuse Reporting Process:

This process will be followed for all security incidents where there are potential breaches of the ICT AUP that require access to detailed user specific monitoring information (other than as detailed in 5.3). It is a formal process but not carried out under the Council disciplinary procedure. Use of any ICT monitoring information for the purposes of investigating potential misuse of ICT, by a specified ICT user, can only be made through the approval process that is relevant to the ICT user. This includes instances where there is an existing disciplinary process underway. This process must also be followed where there is a need for further targeted user specific monitoring to be undertaken.

Once the Potential Misuse Reporting process is instigated, then a Potential Misuse Report must be produced. The format of this and level of detail will be dependent on the circumstances and the agreed scope.

6.4.1 Employees, Contractors and Members

- Approval to proceed with this process will be sought by Council Security personnel from both the Head of Digital Transformation (or delegated representative) and the Head of People & Performance (or delegated representative) for detailed user specific monitoring information to be collated and interpreted. Where the process relates to Members, approval shall also be sought from the Depute Chief Executive. This approval will be documented and retained by ICT Services.
- Once approval has been given, security personnel (Council & in our ICT Providers) will access monitoring information (that has been recorded) or instigate further monitoring that is required to produce the Potential Misuse Report. Any monitoring information may be obtained that is considered to be relevant to the reporting process. The scope will be documented in the Potential Misuse Report.
- A confidential Potential Misuse Report will be produced by the Council Security personnel and authorised by the Head of Digital Transformation (or delegated representative).
- This report will be provided to the relevant Service Director (or delegated representative) and the Head of People & Performance (or delegated representative). This is the end of Potential Misuse Reporting process.

6.4.2 Pupils

- This section relates to Pupils only. Teachers and other school staff, as members of staff as covered in 6.4.1
- Approval to proceed with this process will be sought by Council Security Personnel from the Head of Digital Transformation (or delegated representative) and the Head of Support Services, Care & Learning (or delegated representative) for detailed user specific monitoring information to be collated and interpreted. This approval will be documented and retained by ICT Services.
- Once approval has been given, security personnel (Council & ICT Providers) will access monitoring information (that has been recorded) or instigate further monitoring that is required to report on the incident. Any monitoring information may be obtained

that is considered to be relevant to the reporting process. The scope will be documented in the Potential Misuse Report.

- A confidential Potential Misuse Report will be produced by Council Security personnel and authorised by the Head of Digital Transformation (or delegated representative).
- This report will be provided to the Head of Support Services, Care & Learning (or delegated representative) and the relevant Head Teacher. This is the end of Potential Misuse Reporting process.

7 Management access to ICT user accounts

7.1 Email and Voicemail

If an employee is absent from work and appropriate delegate authority has not been set up, their line manager or higher manager within their management chain may request access in order to achieve continuity of Council business. Attempts by a manager to gain this access for any other purpose will be a breach of the ICT AUP. For example it cannot be used to carry out any form of monitoring. The same applies to voicemail.

The request must be made to the Service Desk. Once the identity of the manager has been confirmed they will be provided with read only delegate access to email and voicemail. No further authorisation is required.

Managers should be aware of their responsibility to only use this access for the purpose of business continuity while the member of user is absent from work. Emails that are clearly personal in nature should not be read. The manager should ensure that they inform the user on their return that delegate access has been obtained. The user may then contact the Service desk to have this removed.

7.2 Network Drive folders and SharePoint storage

If an employee is absent from work and they are holding council information in a network drive folder or SharePoint storage that has access restricted only to them, then their line manager or higher manager within their management chain may request access in order to achieve continuity of Council business. Attempts by a manager to gain this access for any other purpose will be a breach of the ICT AUP. For example it cannot be used to carry out any form of monitoring.

The request must be made to the Service Desk. This will be passed to ICT Services for a governance process to be undertaken. Access will only be given if there is a clear business case provided to justify the access required. This access must be authorised by the Corporate ICT Manager (or delegated representative).

For access to network drive folders and SharePoint storage that are not restricted to a single user, access may be obtained following normal user management processes.

7.3 Network and Business Systems

Network and business system logins are unique to users, and access to logins will not be given to managers as this would be a breach of ICT AUP.

7.4 Legal discovery, Freedom of Information and Subject Access requests

In the event that the Council is legally required to provide access to information held on Council systems to an external person or body then ICT Services may access this information, without the permission or knowledge of users. This could include, but is not limited to, access to email accounts or private areas on network drives and SharePoint.

Whenever possible the user will be informed prior to information being accessed but the Council reserves the right to access information without informing the user, where this is considered to be appropriate in the circumstances. The reasons for not informing the user will be documented by ICT Services.

Authorisation for this access can be given by the Head of Digital Transformation or Corporate ICT Manager (or delegated representative). A Governance process will be followed that ensures that justification for access is checked and recorded and that any decision on whether or not to contact users concerned is also recorded.