Agenda Item	**8**
Report No	**RES/18/21**

HIGHLAND COUNCIL

Committee: Corporate Resources Committee

Date: 8 September 2022

Report Title: **Review of ICT Acceptable Use Policy**

Report By: Depute Chief Executive

1. Purpose/Executive Summary

1.1 This report presents to Members a review of the ICT Acceptable Use Policy (AUP). It was last updated in February 2015. The update does not present significant changes from the previous Policy but does refresh sections in line with some technical enhancements delivered through technology changes leading from COVID and the completion of the ICT Transformation programme and to improve readability.

1.2 The Purpose of the AUP is to provide guidance and clarity on the acceptable uses of ICT to Members; staff; teachers; partner agencies; pupils and anyone else utilising Highland Council equipment; services and applications.

1.3 The AUP is part of a series of policy and guidance documents that support the overall governance of Highland Council that ensures protection of both users and the Council.

2. Recommendations

2.1 Members are asked to:

1. Agree the revised ICT Acceptable Use Policy.
2. Agree that future updates to the ICT AUP are agreed by the ICT Strategy Board and will come back to Committee for approval where necessary.

3. Implications

3.1 **Resource** – No additional resourcing requirements are required to support this Policy. Existing resources in ICT and supporting Services are in place to ensure the Policy is adhered to and communication; induction and training is developed accordingly.

3.2 **Legal** – No specific additional Legal Implication, however this Policy supports other Council Policy's with regards guidance to support General Data Protection Regulation (GDPR) and Computer Misuse Legislation.

3.3 **Community (Equality, Poverty and Rural)** – There are no implications arising from this report.

3.4 **Climate Change/Carbon Clever** - There are no implications arising from this report.

3.5 **Risk** – Approval of this Policy will mitigate risk to the Council and ensure controls and guidance are deployed consistently.

3.6 **Gaelic** - There are no implications arising from this report.

4. Context

4.1 The AUP requires to be regularly reviewed to reflect change of usage patterns; introduction of new technology and the overall risk from Cyber Security threats. This is to ensure that the Council fulfils both its legislative and cultural obligations that can impact both Council ICT user's and the customers/community served.

4.2 The AUP is updated and refreshed through engagement with many stakeholders including Trade Unions; Human Resources, Education and FOI & Data Protection Manager.

5. Policy Updates

5.1 The focus on changes to this AUP was to refresh and update the readability of several sections and to avoid some of the duplication seen in the previous version.

5.2 Since the last review of the AUP, Microsoft Office 365 has been introduced and GSX email services have been removed. This has meant a change in focus from primarily email based guidance to more generic message-based Services. The ability and ease of use of Microsoft Office 365 Products and particularly Microsoft Teams and general file sharing services requires users to consider carefully their actions. The updated AUP reflects this, and guidance has regularly been provided and updated through the ICT Change Network and ICT Toolkit on the Intranet.

5.3 Similarly, in Schools there has been the introduction of Chromebooks and the reduction of Windows managed devices. This has again been reflected in the Policy update and specific guidance has been developed by Education specifically in this area through Digilearn Highland and SharePoint.

5.4 The AUP has a mixture of user advice and guidance and other element that point towards Legal & Disciplinary investigations. Future updates should only require Members approval of the latter. Usage guidance and updates shall be approved by the appropriate Officer Governance established process including the ICT Strategy Board.

5.5 Feedback has been received from Trade Union representatives. Generally, no issues were highlighted although useful comments were made in relation to school pupils, their understanding of the policy and how it is applied in schools. This has not led to a change in the policy, but engagement will continue with Education and Learning colleagues to assist with these points.

Designation:	Depute Chief Executive
Date:	11th August 2022
Author:	Alistair Reid, Interim ICT Operations Manager (Service)

ICT Acceptable Use Policy (AUP) 6.0

Document Control
Version History

Version	Date	Author	Change
1.2	02/02/2000		
1.3	05/02/2010	Judy Wyld/Jon Shepherd/Vicki Nairn	
2.0	11/3/2010	Judy Wyld/Jon Shepherd/Vicki Nairn	
3.0	25/01/2011	Linda Johnstone/John Grieve	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	29/06/2012	John Grieve/Dave Barker	Additional new section (3.12) highlighting potential monitoring of email sent via GSX as a result from the RAP
5.0	21/05/2013	Philip Mallard, Senior Information & Security Officer	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	25/02/2015	Philip Mallard, Senior Information & Security Officer	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
6.0 DRAFT	15/08/2022	Alistair Reid, ICT Operations Manager / Nathan Bates, ICT Officer (Security) / Alexander McKinley, ICT Officer (Security)	Review Updated the document to reflect current legislation, policies and procedures Updated Secure Email section and replaced with Use of Messaging Services section Removed Protective Marking and GCSx references Consolidated sections and improved readability Updates to job titles in line with recent reorganisations Removal of Educational AUP specific references

Document Approval

Name	Title	Role
	Resources Committee	Approval

1 Contents

2 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 Highland Council has to information held on its systems.

3 Scope of the Policy

The Acceptable Use Policy (AUP) applies to all Highland Council employees, agents of The Highland Council, persons representing The Highland Council including sub-contractors and consultants, Partners, Trade Union representatives, Elected Members, and school pupils. For avoidance of doubt, this includes High Life Highland and Valuation Joint Board employees.

This Policy applies to all aspects of ICT use, whether undertaken in a Highland Council location or elsewhere, including the use of any separate standalone systems which are provided by The Highland Council or its ICT providers, the use of personal devices or any ICT used to conduct business on behalf of The Highland Council.

The term ICT covers but is not limited to all Computing Devices, Telephones, Printers and Photocopying Devices and also refers to Information Systems, all Software, Networks, Internet Access, Cloud-based Services and Email Systems.

The Policy statements regarding monitoring of ICT relate to the technical measures in place to monitor activity on Council ICT.

4 Policy Revisions and User Communication

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

5 ICT Acceptable Use Policy Statement

5.1 Expectation of Proper Conduct

The effective operation of The Highland 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 Highland Council Policies.

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 Highland Council or use Highland Council ICT to gain unauthorised access to any other system may be a breach of this Policy and may also be a breach of relevant legislation.

By using any Council ICT Services the user agrees to use it in accordance with this Policy as a

condition of being provided with access to it.

Any 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.

5.2 Dissemination of Information

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

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

The use of this disclaimer does not allow users to undertake any activity which otherwise violates this Policy or any other Highland Council policies or is unlawful activity.

5.3 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 but not limited to following disciplinary processes and procedures or disclosing information to law enforcement agencies.

All users should be aware that use of Council ICT is monitored, and monitoring information is retained and used for both routine security reports and to support potential misuse investigations and enquiries.

Any other ICT users that are not employed by The Highland Council and not subject to The Highland Council disciplinary procedure will be subject to provisions in the contract under which they are providing services. School Pupils will be subject to The Highland Council's promoting positive behaviour policies.

5.4 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 or remit
- Be consistent with The Highland Council Policy, procedure and guidance that is appropriate to any system or network being used or accessed
- Be consistent with appropriate provision and delivery of education
- The handling of the information is appropriate to the type of information that is being accessed or shared
- Is limited personal use as defined in 5.5 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 or remit, including gathering information as part of specific potential misuse reporting or undertaking ICT Security Threat Monitoring

5.5 Personal Use of Council ICT

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

- It is not associated with financial gain relating to non-Council business interests
- 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
- It does not conflict with Council interests

Any questions or guidance about acceptable usage should be discussed with the individual's line manager or teacher for pupils.

5.6 Security

All Users must comply with the Information Security and Assurance Policy (ISAP) which includes but is not limited to the following:

- Not sharing their individual account passwords or allow another person to use their account(s)
- Adhering to Council password standards
- Not using or attempting to use another individual's account
- Not leaving unattended ICT equipment logged on without first locking or logging out of the device
- Notifying the ICT Service Desk and their line manager if they suspect or identify a security problem
- Notifying the ICT Service Desk and their line manager if they suspect a breach of the ICT AUP by any user
- Take reasonable precautions to protect The Highland Council's ICT from security issues such as computer viruses and malware
- Not opening any suspicious email attachments or independently loading any unauthorised software onto their device. If a user does inadvertently open a message or attachment that contains a virus or malware, they should contact the ICT Service Desk immediately0
- Using only properly supplied and authorised applications for undertaking Council business

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

5.7 Unacceptable Use

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

- Restrict or inhibit other users from using the system
- Impair the efficiency of the ICT systems
- Violate or infringe upon the rights of any other person, including the right to privacy
- Act in contradiction to The Highland Council's published Human Resources policies or equivalent

Educational Policies

- Upload, distribute, access or share any material that contains, or can be considered, defamatory, derogatory, abusive, obscene, pornographic, sexually oriented, threatening, racially offensive, otherwise biased, discriminatory or illegal
- Breach legislation or statutory requirements which The Highland Council must comply with
- 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
- Harass an individual or group of individuals
- Create or share any content which breaches confidentiality
- View, transmit, copy, download or produce material, which infringes the copyright of another person, or organisation
- Use the Highland Council internet service or devices to view live TV, TV catch-up services or subscription services where The Highland Council does not have a valid licence
- 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, 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, network controls or any ICT monitoring functions
- Deliberately undertake activities that corrupt or destroy other users' data
- Deliberately undertake activities that disrupt the work of other users, or deny network resources to them
- Violate the privacy of other users
- Send any material that is sensitive personal data or confidential or valuable data that would be considered so by The Highland Council to unsecure external addressees or contacts without prior authorisation from information owners
- Attempt to alter or tamper with the ICT provided to them.

5.8 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.
The system, however, is not fail-safe and the Highland Council cannot prevent the possibility that some sites are accessible which have not been detected by our systems and are inconsistent with the policies of The Highland Council.

Where material which is not consistent with the policies of The Highland Council is inadvertently accessed, users must report the matter to their line manager and to the ICT Service Desk immediately or to a teacher for pupils.

5.9 Use of Messaging Services

Externally addressed email (initiated through Microsoft 0365; Outlook; Teams or SharePoint) is often not secure. However, the Council, along with most Public Sector organisations, are

committed to deploying Government guidance and controls to ensure security risks are mitigated. Any material that is sensitive personal data, confidential or valuable to The Highland Council should not be emailed externally unless through or to a secure and trusted source. For communication with some partners secure email is available through the normal Highland Council email system. Most emails will automatically send through a secure transmission method. Users should manually encrypt emails, using standard features in Outlook, to send any sensitive data. It should be assumed that it is not secure to send emails to any organisation or individual that is not identified as having secure email. If you are in any doubt about the security of email, then you must seek advice from your line manager before sending the email.

Particular care should be taken when using the “reply to all” function and when checking the recipients in a mail distribution list or groups prior to communicating through a messaging service. Users should use BCC when widely distributing information to protect individual’s personal data, i.e. email addresses.

If a member of the public requests their personal data to be emailed to them, then this can be done when they confirm that they accept the risk of receiving their personal data over an unsecure email connection. If this involves sensitive personal data, then this permission must be confirmed 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.

Email 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.

6 Monitoring Usage of ICT and User Activity

6.1 Overview of Council Monitoring

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

The Highland Council uses monitoring and filtering tools that will block access to some websites. If access to a blocked site is required for business reasons, then this may be requested, and any such request will be subject to an ICT governance process. Any attempt to circumvent such restrictions will constitute a breach of the ICT AUP.

To ensure compliance with this Policy, The Highland Council also reserves the right to use monitoring software to check upon the use and content of messaging services. Such monitoring is for legitimate purposes only and could be used to check for any rude or offensive words or phrases.

If there is reason to suspect that there has been improper use of ICT services by a specified 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 The Highland Council’s Human Resources Policies.

Users should be aware that any email that leaves Council systems and any internet usage may be monitored by external bodies such as internet service providers (ISP).

6.2 ICT Security Threat Monitoring

The Highland 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 Highland Council's network or infrastructure, with the permission of the Head of ICT & Digital Transformation or the ICT Operations Manager, monitoring information shall be used by ICT security personnel to identify more information on the threat and to enable a prompt response to be made. Where necessary to understand the threat, this will also 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 the follow-up action will be to instigate the approval process as set out in The Highland Council's Human Resource Policies. This information will be used to create a Potential Misuse Report.

7 Information Security Incidents and Potential Misuse Investigation

7.1 Information Security Incident Management Process

ICT Services manages Information Security incidents. This includes potential breaches of the ICT AUP as well as security concerns that may not be related to user misuse. The ICT Security Operations team ensures a consistent approach is taken when reviewing each security incident.

7.2 Information Security Incident Identification and Logging

Any user can raise an information security incident by calling the ICT 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 ICT 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.

7.3 Evaluation of Security Incidents

ICT Services will use the information provided as part of the logging of the security incident to determine 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 contacting 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 involves a potential breach of Data Protection legislation, then the relevant Information Asset Owner (of the information involved in the breach) may 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.

7.4 Potential Misuse Process:

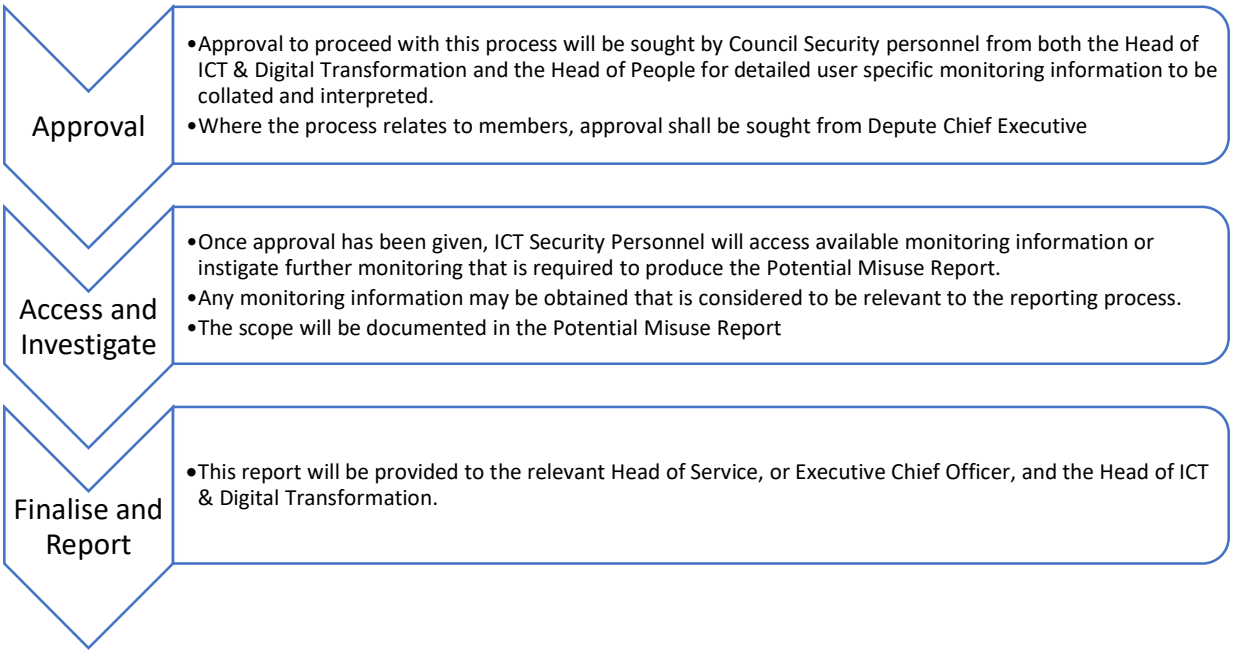
The potential misuse process is initiated when ICT Services either receive an automated notification of a security incident, a request from Human Resources or when a user reports potential misuse via the ICT Service Desk.

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. Use of any ICT monitoring information for the purposes of investigating potential misuse of ICT, by a specified user, can only be made through the approval process that is relevant to the ICT user group outlined below. It is a formal process but not carried out directly under The Highland Council disciplinary procedure. However, instances where there is an existing disciplinary process underway, the potential misuse report can run simultaneously.

Once the Potential Misuse Reporting process is instigated, then a Potential Misuse Report must be produced.

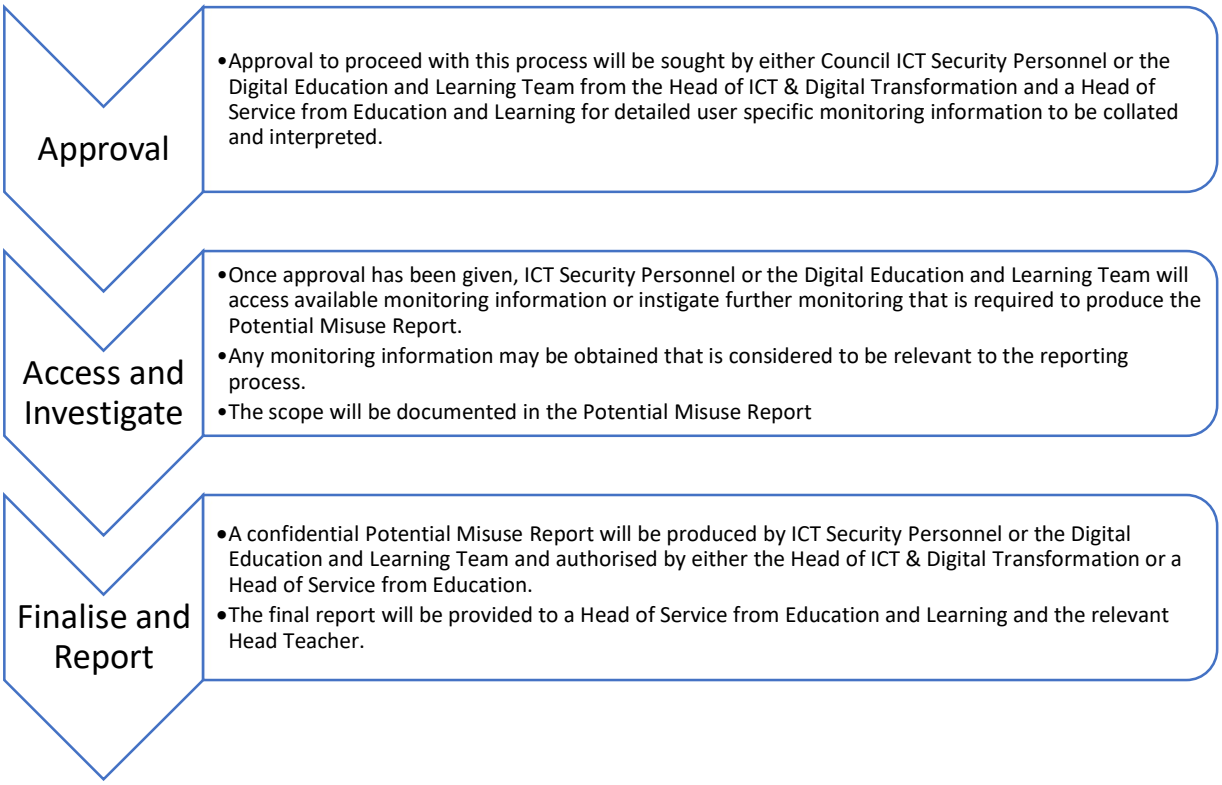
7.4.1 Employees, Contractors and Members

- Approval to proceed with this process will be sought by Council Security personnel from both the Head of ICT & Digital Transformation and the Head of People for detailed user specific monitoring information to be collated and interpreted. In the absence of either Head of Service, approval will be obtained from the relevant Executive Chief Officer that they report to.
- 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, ICT Security personnel will access available monitoring information 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.
- This report will be provided to the relevant Head of Service, or Executive Chief Officer, and the Head of ICT & Digital Transformation.



7.4.2 School Pupils

- Approval to proceed with this process will be sought by either Council ICT Security Personnel or the Digital Education and Learning Team from the Head of ICT & Digital Transformation and a Head of Service from Education and Learning for detailed user specific monitoring information to be collated and interpreted.
- Once approval has been given, ICT Security Personnel or the Digital Education and Learning Team will access available monitoring information or instigate further monitoring that is required to produce the Potential Misuse Report. Any monitoring information may be obtained that is relevant to the reporting process. The scope will be documented in the Potential Misuse Report.
- A confidential Potential Misuse Report will be produced by ICT Security Personnel or the Digital Education and Learning Team and authorised by either the Head of ICT & Digital Transformation or a Head of Service from Education.
- The final report will be provided to a Head of Service from Education and Learning and the relevant Head Teacher.



8 Management Access to ICT User Accounts

8.1 Network and Business Systems

Network and business system logins are unique to users, and access to specific user login information will not be given to managers as this would be a breach of ICT AUP. Instead, access may be provided to information stores that are only accessible to an individual user to ensure business continuity.

8.1 Access to Individual Systems for Network, Email, Voicemail and File Storage

If an employee is absent from work and an appropriate delegate authority has not been set up for access to said individual's Network, Email account, Voicemail or File Storage, their line manager or higher manager within their management chain may request access to achieve continuity of Highland Council business. Attempts by a manager to gain this access for any other purpose will be a breach of the ICT AUP. This access cannot be used to carry out any form of employee monitoring.

The access request must be made to the ICT Service Desk. Once the identity of the manager has been confirmed they will be provided with read only delegate access to the required systems. 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 or user is absent from work. Documents or 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 manager should then remove this delegate

access or contact the ICT Service Desk to have the access removed.

If access is required to stores that had access restricted to a former member of staff, then full read and write access may be provided to the manager. The manager may use this access to review, file and delete documents as appropriate in accordance with the Records Retention & Disposal Policy.

For access to storage that is not restricted to a single user, access may be obtained following normal user management processes via the ICT Catalogue.

8.2 Legal Discovery, Freedom of Information (FOI) and Subject Access Requests

In the event that the Council requires access to information held on Council systems for its own legitimate purposes, or it is legally required to provide access 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. Authorisation for this access can be given by the Head of ICT & Digital Transformation and the Head of Corporate Governance. In the case of an FOI or Subject Access Request, this should be confirmed by the FOI and Data Protection Officer.

9 Related Council Policy and Standards

The below policies can be found within **The Highland Council Intranet**

- Policy on the Acceptable Use of Social Media
- Information Security & Assurance Policy
- Information Management Policy
- Data Protection Policy
- Records Management Policy
- Records Retention & Disposal Policy
- Education and Learning Policies
    - Promoting Positive Relationships Framework and Guidance 2021
    - Chromebooks
    - GTC Professional Guidance on The Use of Social Media
    - Highland LNCT Disciplinary and Grievance Procedures
- Relevant HR Policies
    - Equal Opportunities Policy
    - Disciplinary Procedures
    - Whistleblowing
    - Councillors Code of Conduct
    - Staff Code of Conduct