The Highland Council

Agenda Item	17
Report No	**FHR/ 82/13**

Finance, Housing and Resources Committee
5 June 2013

Review of ICT Acceptable Use Policy

Report by Assistant Chief Executive

Summary

This report informs members of the changes introduced as part of the review of the Council's ICT Acceptable Use Policy and requests the Committee to consider and approve the revised ICT Acceptable Use Policy (AUP).

1 Background

1.1 This cover report provides a summary of changes introduced as part of the review of the ICT Acceptable User Policy (AUP) referred to in Annex A.

1.2 The 'Policy on the Acceptable Use of Information Systems, Communications and Technology' was originally approved by the Resources Committee in March 2010.

1.3 Therefore the Policy is due for a review and internal audit review has highlighted best practice areas for improvement in the policy, in particular, to set out more clearly the ICT monitoring that the council undertakes, and these have been incorporated.

1.4 The title has been changed to ICT Acceptable Use Policy (AUP), to reflect the name that it is widely known by and follows the standard title used for this type of policy.

2 Policy Scope

2.1 The updated AUP sets out more clearly which end users are within the scope of the policy. The wording has been changed to confirm that 'all Council users' includes pupils.

2.2 Public Users of Council ICT such as library users have been removed from scope as a separate AUP is already in place to cover this. Highlife Highland has an Internet Acceptable Use Policy for the use of computers, the internet and email, and this is available to their users on their website.

3 Policy Structure

3.1 The AUP has been restructured to more clearly set out how ICT usage is monitored, and how monitoring information may be used.

3.2 There is a new section which sets out the Council's right of access to information held on storage devices and in ICT accounts. The council is required to access and disclose information through legislation such as the Freedom of Information (Scotland) Act 2002 and Data Protection Act 1998. This update to the Policy is intended to clarify the situation for users and ensure there is a clear approach within the Council to accessing information that the council is legally required to access and disclose.

3.3 Despite these changes to structure the overall Council Policy on what is acceptable and unacceptable use of ICT has not changed significantly as a result of this update to the policy. The changes to the policy that have been made are set out below.

4 Changes to the Acceptable Use Policy Statement

4.1 Following advice from Internal Audit, reference has been added in the document to the Computer Misuse Act 1990. In addition to this there will be an update to the log-in message for all PC / laptop ICT users to refer to the Act.

4.2 The policy has been amended to reflect the use of the Council ICT within an educational setting, such as referring to sanctions for misuse by school pupils and recognising that appropriate use includes the provision of education.

4.3 A new section has been created for personal use of Council ICT. The existing policy covers this but this structural change has given greater visibility to this. The change does not alter the policy position and continues to allow personal use outside of work hours.

4.4 A new reference has been added to set out that unacceptable use includes any attempt to bypass the Council internet filtering or any ICT monitoring functions.

4.5 The section on unacceptable use has been updated to highlight that the items of unacceptable use listed are examples rather than an exhaustive list and that each incident of potential misuse will be considered on its individual circumstances.

4.6 Updated reference to sending personal information via email has been added to reflect new guidance the council has received from the Information Commissioner. This confirms that the council may permit personal information to be sent via normal email (unencrypted) to a customer if the personal data is that of the customer, the customer is aware of the risks and has specifically requested that the council do so. The changes provide some guidance to staff on the assessment that must be made prior to any personal data being sent by email and subject to this being followed permit the transmission.

4.7 The approvals for access to ICT monitoring information have been strengthened and made more appropriate to the different types of ICT users.

As with the current policy the Head of E-Government and Head of HR must provide their approval for a potential misuse investigation. The updated policy now requires additional approval from the Assistant Chief Executive for potential misuse investigations into Members usage, and from the Head of Support Services (ECS) for pupils. The Policy continues to allow for delegates to be nominated for each of these approvals to ensure business continuity.

5 Social Media Acceptable Use

5.1 The Social Media Acceptable Use Policy and Guidance that was agreed at the January and April Finance, Housing & Resources Committee supports the ICT AUP.

5.2 The ICT AUP sets out what constitutes unacceptable behaviour when using the internet and includes specific reference to accessing and contributing on Social Media when using council ICT and when acting on behalf of the council.

5.3 The Social Media AUP sets out how staff and members can use Social Media in their personal, professional and council lives in a way that is consistent with the ICT AUP and other council Policies and codes of conduct.

5.4 The updated ICT AUP refers to the Social Media AUP in the section that sets out how usage is identified as being acceptable.

6 Communication & Implementation

6.1 To promote awareness of the policy change and improve staff awareness of acceptable and unacceptable use there will be a range of communication and awareness raising approaches used.

6.2 Staff and Elected Members will be informed of the updated policy through an All User email and publication of the updated policy on the Council Intranet and highland.gov.uk website.

6.3 This will be supported by cascading of key messages through the new Information Management Governance Board that will have senior representatives from each service within the council.

6.4 Updated simplified acceptable use documents will be issued for school pupils and Head Teachers will be supported in the communication of this by ECS.

6.5 ICT users will be informed of the updated AUP through an update to the log-in message on Council PCs and Laptops.

7 Implications

7.1 **Legal & Risk:** The changes to the policy provide ICT users with improved information on the ICT monitoring that the council undertakes, which is necessary to support compliance with the Data Protection Act 1998. This and the inclusion of a reference to the Computer Misuse Act 1990 in the Policy and log-in message have been made on the advice of Internal Audit.

7.2 **Resource:** The changes to the policy introduce additional authorisation for access to ICT monitoring information, but additional resources will not be required to operate with this change. Communication and Implementation will be carried out using existing resources.

7.3 **Finance:** There are no implications arising from this policy review.

7.4 **Equalities:** The changes to the policy do not have a detrimental effect on any particular group.

7.5 **Climate Change:** There are no implications arising from this policy review.

Recommendation

Members are asked to:

1) Note the changes within the revised ICT Acceptable Use Policy
2) Approve the ICT Acceptable Use Policy (Annex A)

Designation: Senior Information & Security Officer
Date: 21 May 2013
Author: Philip Mallard

Background Papers: ICT Acceptable Use Policy (AUP)

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	DRAFT	21/05/2013	Philip Mallard, Senior Information & Security Officer	DRAFT	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).

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 will be made available for pupils of different ages to promote understanding of the behaviours that are expected of them as well as acceptable / unacceptable use. It is the responsibility of Head Teachers and Teachers to ensure that all pupils within their school are aware of this policy and understand their responsibilities.

The term ICT covers all computing devices (including mobile devices), telephones (including mobile phones), printers and photo copying 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 the 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 you must only use ICT that you have been authorised to 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 you agree 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 Services, legal action or involvement of law enforcement agencies. You should be aware that use of council ICT is monitored at all times and monitoring information is retained to support investigations into potential misuse.

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 to 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**

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. lunchtimes, before or after work)
- is not interfering with the delivery of the Highland Council services
- does not violate this or any other Highland 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 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 Highland Council business
- 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 Highland Council ICT system or device which connects to the council network or is operated by the council (or a Council managed organisation) 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 Highland 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.
- 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 / confidential 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 incident would be assessed on its individual circumstances. If you are in any doubt about what constitutes acceptable or unacceptable use you should seek clarification from your 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.

Externally addressed email is often not secure. Any material that is sensitive / confidential personal data, confidential or valuable to the Council should not be emailed externally unless encrypted or sent through a secure service. For communication between some government agencies secure email can be achieved through use of the Government Secure Extranet. 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 aware of the risk and confirm in writing that they want to accept that risk. 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 the Council's 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"

5 Monitoring usage of ICT and user activity

5.1 Council monitoring

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

The Highland Council's ICT equipment and resources are provided for 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, email usage, internet usage, telephony usage and ICT usage is recorded and retained by the Highland 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 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 AUP. Should access to a blocked site be required for business reasons any such request will be subject to an ICT governance process.

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.

Reports on ICT usage (including email) may be provided to 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 AUP, but if there is no business reason for this it could justify further investigation (following the procedure for investigations into potential misuse).

If routine monitoring identifies user activity that could constitute a breach of AUP then this will be logged as a security incident by ICT Services.

If there is reason to suspect that there has been improper use of ICT, further 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 GSX Interception & Monitoring

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

5.3 Other external interception & monitoring

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

6 Information Security Incidents and potential misuse investigations

6.1 Information Security incident management Procedure

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

ICT Services will produce and maintain a procedure for the management of Information Security incidents. This includes potential breaches of the AUP as well as security concerns that may not be related to user misuse eg malware. It ensures a consistent approach to reviewing each security incident. Changes to this operational procedure will be agreed by the Head of e-Government. A copy of the current procedure will be made available to staff on the intranet

The approach to investigations is similar for all ICT users within the scope of this policy, but there are different senior managers involved depending on the type of user. The following sections set out any variations.

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 AUP.

All information security incidents raised through the Service Desk will be evaluated by ICT Services but not all information security incidents will result in an investigation into potential misuse, dependent on the severity of the breach and the circumstances. ICT Services will keep records of all reported incidents.

6.3 Evaluation of incidents

The 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 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 AUP. If there is insufficient information then the users involved may be contacted by ICT Services to identify further information and full cooperation with this must be provided by users. At this stage monitoring information will not be accessed.

If the circumstances make contact with the users involved difficult or inappropriate then a Potential Misuse investigation may be carried out to enable access to monitoring information.

If the incident may have resulted in a breach of the Data Protection Act 1998 then a potential misuse investigation will be instigated and the user(s) involved and/or their manager will be required to complete a Data Protection Breach Report.

6.4 Potential Misuse Investigation:

This will be used for all potential breaches of AUP that require access to monitoring information. 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 can only be made through the approval process that is relevant to the user. This includes instances where there is an existing disciplinary process underway.

6.4.1 Employees and Contractors

- Approval to proceed with this investigation will be sought by ICT Services from both the Head of E-Government (or delegated representative) and the Head of HR (or delegated representative) for specific monitoring information to be obtained and evaluated. This approval will be documented and retained by ICT Services.
- Once approval has been given, ICT Services will access monitoring information that has been recorded or instigate further monitoring that is required to investigate the incident. Any monitoring information may be obtained that is considered to be relevant to the investigation. The scope of the investigation will be documented and retained by ICT Services.
- A confidential monitoring report will be produced by the Corporate ICT Manager (or

delegated representative) and authorised by the Head of E-Government (or delegated representative).
- This report will be provided to the relevant Service Director (or delegated representative) and the Head of HR (or delegated representative).

6.4.2 Elected Members

- Approval to proceed with this investigation will be sought by ICT Services from the Head of E-Government (or delegated representative), Head of HR (or delegated representative) and the Assistant Chief Executive (or delegated representative) for specific monitoring information to be obtained and evaluated. This approval will be documented and retained by ICT Services.
- Once approval has been given, ICT Services will access monitoring information that has been recorded or instigate further monitoring that is required to investigate the incident. Any monitoring information may be obtained that is considered to be relevant to the investigation. The scope of the investigation will be documented and retained by ICT Services.
- A confidential monitoring report will be produced by the Corporate ICT Manager (or delegated representative) and authorised by the Head of E-Government (or delegated representative).
- This report will be provided to Assistant Chief Executive (or delegated representative) and Head of HR (or delegated representative).

6.4.3 Pupils

- Approval to proceed with this investigation will be sought by ICT Services from the Head of E-Government (or delegated representative), the Head of HR (or delegated representative), and the Head of Support Services, Education, Culture & Sport Service (or delegated representative)for specific monitoring information to be obtained and evaluated. This approval will be documented and retained by ICT Services.
- Once approval has been given, ICT Services will access monitoring information that has been recorded or instigate further monitoring that is required to investigate the incident. Any monitoring information may be obtained that is considered to be relevant to the investigation. The scope of the investigation will be documented and retained by ICT Services.
- A confidential monitoring report will be produced by the Corporate ICT Manager (or delegated representative) and authorised by the Head of E-Government (or delegated representative).
- This report will be provided to the Head of HR (or delegated representative) and Head of Support Services, Education, Culture & Sport Service (or delegated representative).

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 the 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 AUP. For example it cannot be used to carry out any form of monitoring.

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 the line manager or higher manager within the 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 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).

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 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 e-Government 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.