Electronic Communications Policy
City of York Council

Issue Date: October 2022
Version: 8.

Contents

Attention: This document is uncontrolled when downloaded or printed! Please be advised that the policies, regulations and procedures in this document are subject to change without prior notice, if necessary, to maintain compliance with current legislation and/or with rules and regulations as directed by the ICT Department Management Team (DMT) and/or CYC Corporate Management Team (CMT). To ensure compliance with the most current version of this policy please be sure to review it regularly.

Current Document Status

Approving Body: ICT DMT
Date of Formal Approval: April 2020
Responsible Officer: Head of ICT
Document Retention Period: Until Superseded

Version History

Date	Version	Reviser	Comments
Mar 2017	6.0	Head of ICT	Minor amendments
June 2017	6.1	ICT Security Officer	New front cover + document control layout
July 2017	6.2	ICT Security Officer	Updated references to other policies (section 4.2)
May 2018	7.0	ICT Infrastructure Manager	Major update GDPR
April 2020	8.0	ICT Infrastructure Manager	Section 6 added for Audio visual meeting products
July 2020	8.1	ICT Security Officer	Ported to Markdown
July 2020	8.2	ICT Infrastructure Manager	Review and minor changes
July 2020	8.3	ICT Infrastructure Manager	Added subsection to cover staff profiles in Delve

Review History

Review Period: 24 months

Date Reviewed
March 2020
October 2022

Principle

City of York Council (CYC) is committed to using information technology, computer systems and all electronic forms of communication in a secure, efficient and legitimate manner.

Ensuring the effective use of these communication tools is essential in order to manage their impact on CYC's ICT infrastructure, make optimal use of ICT resources, protect CYC's reputation and mitigate the risk of abuse to and from its staff and elected members. Whilst it is recognised that staff have the right to carry out their duties in a dignified manner with respect for their privacy and autonomy, this needs to be balanced against the protection of CYC's interests. The protection of CYC's reputation and its employees is a critical responsibility for each individual within the organisation and for the organisation as a whole.

The Electronic Communications Policy (ECP) sets out how CYC employees should use information technology, computer systems and all electronic forms of communication appropriately in the workplace. The ECP applies to all information technology users, whether working within a CYC building or remotely, including staff, Elected Members and third parties.

This policy must be communicated to all Information technology users and will apply to all users of CYC's infrastructure whether accessed from within a CYC building or remotely. Managers have a key responsibility in ensuring adherence to this policy and must discuss the requirements with their staff to ensure compliance within their Directorate, department or team. This policy will be reviewed on a biannual basis to take into account changes in legislation, instances of abuse or misuse and concerns from staff and unions.

Particular emphasis will be placed on ensuring that all users of Information Technology and electronic communication tools are fully aware of:

- Appropriate and inappropriate use of CYC's Information Technology facilities;
- What constitutes misuse or abuse (whether accidental or intentional); Misuse can be a criminal offence. To avoid misuse employees should not:
- Send anything that could be interpreted as abusive, intimidating, malicious or insulting.
- Intentionally access material which is offensive or illegal via the internet or email.
- What constitutes offensive material or harassment through the use of Information technology and electronic communications facilities.
- Use which would bring CYC's name into disrepute.
- Their responsibility for use and security of data they use in the execution of their duty and their own user login details and passwords;
- Their responsibility for the security of all data held by CYC

Effective Date

This policy is effective on 1st April 2020.

Approval Status

This policy was originally prepared by ICT and approved by the Corporate Information Governance Group.

Scope

This policy applies to:

- All CYC employees engaged in work for the council including those working from council buildings, home, non-Council locations or working remotely;
- Any other use by CYC employees which identifies the person as a CYC employee or which could bring it into disrepute and create a liability for CYC;
- Other people working for, or engaged on, CYC business or using CYC ICT equipment or infrastructure including third party and partner organisations;
- Elected members.

The Director of Children , Education and Communities recommends the policy for adoption by school governing bodies to include schools staff that use ICT facilities and are employed by CYC.

This policy applies to the use both acceptable and inappropriate of ICT equipment including but not restricted to e-mail, instant messaging, social media, internet, telephones (including Smartphone's and other mobile phones) and voicemail. It applies to use of CYC provided equipment and authorised personal equipment such as fax services, copiers, scanners, CCTV, and digital security key fobs and cards.

Electronic Communications and the Law

Misuse of the Internet, E-mail, telephony, mobile or ICT equipment can constitute a criminal offence (e.g. Sexual Offences Act 2003, Computer Misuse Act 1990). Where CYC believes a criminal offence has taken place, it is the duty of the Director of the employing department, in consultation and in accordance with advice from the Head of Human Resources and the Head of ICT to inform the police. Alternatively, based upon the nature of the misuse and its implications, the Head of Human Resources and/or the Head of ICT could initiate this process and advise the relevant Director.

In such cases, individual staff may be subject to prosecution and CYC and the individual could be liable to pay damages. Using CYC's facilities illegally constitutes gross misconduct and will result in the instigation of the CYC's disciplinary procedure.

Systems and Data Security

Information Storage

Computer and electronic storage is expensive and corporate or local based storage facilities must not be used to store large amounts of personal data. This places an unnecessary burden on the corporate storage and network services, increases system backup and restore times and may affect the recovery time in the event of a disaster

recovery situation. Local management must ensure that storage is periodically reviewed and data no longer required is deleted in order to make best use of the resource and keep costs to a minimum.

In order to comply with the General Data Protection Regulations, the Data Protection Act and other appropriate legislation the following MUST be complied with when storing personal or personally identifiable data. All such data:

- Must be stored in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, alteration, destruction or damage
- Must be stored on corporate storage where it can be searched, indexed, disclosed as part of a legal request and deleted (i.e. not in personal home areas)
- Must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is being kept or processed
- Must be accurate and, where necessary, kept up to date
- Must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is required either for processing or to comply with legislation
- Must be covered by a retention policy

Information Management

This policy should be applied with due regard to the following council policies concerning information management:

- Information Management
- Data Protection Policy
- Freedom of Information Policy
- Records Management Policies (corporate and departmental)
- CYC ICT Information Systems Security and Acceptable Use Policy
- CYC ICT Laptop Usage Policy
- CYC ICT Mobile and Remote Working Policy
- CYC ICT Information Security Incident Management Policy
- CYC ICT PSN Acceptable Usage Policy and Personal Commitment Statement
- CYC ICT Global Email Policy
- Social Media Policies
- CYC ICT Third Party Access Policy
- Any other relevant policies as advised from time to time.

All electronic documents including emails should be prepared in the expectation that they may be disclosed to individuals whose personal data they contain, or to the public at large. They should therefore be factual and objective, up to date and avoid inappropriate and offensive language, or evidence of any sort of prejudice. Opinions, if recorded at all, must be professional and defensible.

All electronic documents including emails should be created, stored, closed and destroyed in accordance with relevant business defined records management policies to comply with all appropriate UK legislation including, but not limited to, the General Data Protection Regulations and the Data Protection Act. These must ensure availability for quick and easy location and retrieval. The use of personal "home" areas (inaccessible to colleagues or managers) should be reserved for documents that are in fact personal in

nature. The following are examples of the type of information that could be stored within the individuals "home area":

- Flexi sheets
- Appraisal notes
- Correspondence with unions or other advisers
- Work in progress (WIP) when formulating ideas/plans prior to distribution
- Disciplinary notes

This information could also relate to others for those staff with line management responsibility.

Note that if elected members or staff employees include personal data in their home area, they may qualify as "data controllers" under the data protection act and therefore be liable for the content. In such cases CYC will not be responsible for the associated obligations under the Data Protection Act; no processing is permitted which might create a liability on the CYC.

Personal documents may be retrieved by electronic searches in response to requests for information, and if so, will be inspected as part of the decision around disclosure or exemption in accordance within the Freedom of Information Act.

Do:

- Prepare all electronic documents in a professional manner. Be factual and objective and avoid inappropriate or offensive language.
- Create, store, close and destroy electronic documents in accordance with the relevant records management policies.
- Use the "home area" for personal documents, such as appraisal notes, disciplinary notes or correspondence with unions.
- Create a retentions policy and assign it to all data for which you are the data owner.

Don't:

- Store large amounts of personal data on a PC or other corporate storage facilities.
- Keep documents, emails or other electronic documents longer than necessary.
- Share any data with any other party, internal or external to the council, without the data owners permission and only with parties for which there is a valid data sharing agreement in place.

Anti-Virus

CYC's anti-virus system provides a business class level of proactive protection including the automatic update of the latest anti-virus files for the central corporate infrastructure. This includes any PC, laptop or other Information technology equipment that connects to the corporate network either from the office or remotely e.g. from home. The same anti-virus solution is also used to reduce the potential risk posed from the use of portable storage items including DVD, memory sticks etc.

Staff and Elected members who have a PC, Laptop or other device provided by CYC that does not connect to the corporate network (i.e. stand alone laptop, PC or tablet) are responsible for ensuring it remains virus-free. They are responsible for the security and integrity of the device and all data stored on it, and this includes the use or access by non-authorised persons.

Users must contact the ICT Service Desk immediately if they suspect that the security or integrity of the PC/Laptop/device has been compromised, for the necessary checks to be carried out.

Knowingly infecting the ICT infrastructure or any device with a virus by acting in a reckless or malicious manner that puts the infrastructure at risk constitutes gross misconduct and will trigger the CYC's disciplinary procedure

Network Security

Staff and Elected Members must not physically connect any device that is not CYC registered onto the corporate infrastructure – i.e. bring non CYC equipment into a CYC office and physically plug it into the network. Doing so will be treated as a serious breach of this policy.

If in doubt, you must contact the ICT Service Desk so that an assessment can made of any potential threat to the councils infrastructure or information integrity or availability. ICT reserve the right to deny any device access to the corporate network if it does not conform to the required security standards.

ICT Support Services has robust procedures and processes in place to mitigate the risks of the corporate infrastructure being compromised. To help sustain these, elected members, staff and third parties must not attach a CYC supplied and registered device to a network port that has not been expressly identified for the purpose or unplug any non-portable network device from the network.

Any proposed moves or change requests involving the corporate network must be reported to the ICT Service Desk so that adequate preparation and security implications can be assessed and applied.

ICT will apply approved and appropriate updates and software patches to all networked devices as they become available. Elected members, staff and third parties must not refuse to accept or knowingly remove such updates, patches or applications.

Staff and Elected Members must not:

- Seek to gain access to restricted areas of the CYC network;
- Access or try to access personal or management data unless legitimately authorised to access such material as part of work duties. If in any doubt, seek the authorisation of your line management;
- Perform personal searches beyond the acceptable use criteria;
- Intentionally introduce any form of malware program (e.g. computer virus);
- Carry out any hacking activities;
- Upload any software to the internet or other external networks without prior notification and authorisation from the ICT Service Desk.

Under no circumstances should users download or install software without prior notification and authorisation from the ICT Service Desk. Appropriate action will be taken against any user found to have installed software that is not properly licensed or if the software is being used contrary to its license agreement.

Users must not attempt any technical maintenance on any CYC computer systems or

networks (e.g. adding addition RAM); this must be carried out by ICT only.

E-mail Use

Etiquette and Content

CYC's email system is an effective method for supporting the delivery of its services. As with any other form of communication, care and consideration must be taken in its use. The use of email as a communications tool requires particular care. The recipient could easily misinterpret the informal nature, including language and tone and the consideration of whether e-mail is the appropriate method for a particular communication should be taken into account.

In order to protect the interests of CYC, its Elected members and its staff, agents and representatives, the following standard disclaimer is added automatically to all external emails (whether business or non-business related) at the point that they are sent.

It is not permitted under any circumstances (except with the prior written approval of the Head of Legal services) to make additions to, alter, amend or delete any part of this disclaimer. This applies to any addition, alteration, amendment or deletion whether directly, indirectly or by explicit or implicit reference.

CYC's standard disclaimer is:

> *This communication is from City of York Council. The information contained within, and in any attachment(s), is confidential and legally privileged. It is for the exclusive use of the intended recipient(s). If you are not the intended recipient(s), please note that any form of distribution, copying or use of this communication, or the information within, is strictly prohibited and may be unlawful. Equally, you must not disclose all, or part, of its contents to any other person. If you have received this communication in error, please return it immediately to the sender, then delete and destroy any copies of it. City of York Council disclaims any liability for action taken in reliance on the content of this communication.*

Elected Members and Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager OR the Human Resources Department.

Elected Members and Staff should take care with the content of e-mail messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Users should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not necessarily mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable.

In general, users should not:

- send or forward private e-mails at work which they would not want a third party to read

- send or forward chain mail, junk mail, cartoons, jokes or gossip
- contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them
- sell or advertise using our communication systems
- agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;
- download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;
- send messages from another worker's computer or under an assumed name unless specifically authorised; or
- send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

To avoid becoming the victim of 'phishing' attacks (a fraudulent attempt, to steal personal information, such as user names, passwords or bank details) do not follow links embedded in emails, but instead type in the URL, you have checked as correct, into the browser bar, or use a saved URL if navigating to a favourite site such as a bank or online store. Elected Members and staff who receive a wrongly-delivered e-mail should return it to the sender and delete it.

Personal Use

CYC recognises that there will be occasions when elected members and staff need to send/receive personal emails. Occasional and reasonable personal use is permitted providing that:

- It does not interfere with the performance by staff of their duties,
- It is undertaken in their own time,
- It does not harm the performance of the email system or the corporate network,
- It is not for furthering outside business interests or for personal monetary gain
- The email conforms to all other requirements of this policy.

Receipt of illegal spam

CYC's anti spam system should stop elected members and staff from receiving junk mail, offensive or sexually explicit material. This form of malicious activity is constantly changing and evolving, some offensive or sexually explicit material may get through the anti spam system. In such cases, elected members, staff and third parties must inform the ICT Service Desk immediately and in doing so will not be held responsible for the content. Once informed, ICT will manage the incident through the nationally established procedure for reporting illegal content specially aimed at child abuse images worldwide, criminally obscene content and criminally racist content.

Misuse of CYC's email service is a violation of this policy. The nature of the misuse will determine the subsequent action to be taken including disciplinary proceedings.

External E-mail

Users are expected to conduct themselves appropriately and in a manner which is consistent with their CYC contract of employment, following all CYC policies and procedures, relevant legislation and good practice guidance.

Email Storage

Email messages and content can constitute personal data and must be treat in the same way as any other personal data following the same principles as those under the data storage section of this policy (Section 4.0). This includes both the content of the message and the email address sent from or to. Email addresses consisting of firstname, lastname and company name for example can clearly be used to personally identify the individual and must be treat as, stored and protected in same way as any other personal data. Before disclosing the data you must have positive consent to share this information from the data owner so must take care when forwarding or distributing such messages.

Emails must not be stored in pst files or off line storage areas under any circumstances. They should also not be stored in areas that are not backed up, part of a data retention policy, not index-able or not search-able.

Corporate Profiles (Delve)

Profile Data

All photos that are uploaded for the purpose of a user profile should remain professional where the focus is maintained on the face, with appropriate attire, the only subject in the photo should be the employee and not contain images that do not represent the employee.

To ensure accuracy of information, staff should update their profile regularly to reflect their working responsibilities.

ICT must be updated when an employee moves team or department so that the core data linking to a profile is correct and up to date.

Audio Visual Conferencing and Instant Messaging

Platforms

Meetings and conferences at which City of York Council business will be discussed must not be hosted on platforms that are not approved or supported by CYC ICT.

Etiquette and Content

The same rules apply when using audio visual and instant messaging platforms as those for email.

All content whether verbal, visual or text should be accurate, relevant and appropriate and in strict compliance with the same rules pertaining to email content. The content should not be recorded, copied or forwarded to any other party without the express permission of all parties involved in the conference.

When working from outside or inside the office care should be taken to ensure that no content is visible or audible to people not directly involved in the conference. This can best be achieved by the use of headset and microphone, ensuring you are in a quiet

location and fully aware of your surroundings.

If the file sharing functionality of the platform is active you should not share files that are of a sensitive nature without being fully aware of who the recipient is and without clearly

defining what the recipient can and cannot do with that data in accordance will all other policies and data sharing agreements.

If screen sharing functionality is available in the platform then care must be taken when using this so that there are no sensitive emails, documents or other data not relevant to the meeting is visible on the desktop before presenting a desktop

All conversation and content shared on a platform may be stored and searchable for the purposes of ensuring compliance with all CYC policies, Freedom of Information Requests legal and disciplinary purposes. It should not be assumed that anything communicated on such a platform is private.

Security

You are responsible for assessing whether the platform you are proposing to use for conferencing and message is secure enough for the information you are intending to share, especially personal and confidential information. If in doubt ask ICT for advice.

You should notify meeting participant before conferencing and messaging, that the third-party application being used could potentially introduce privacy risks.

Wherever possible you should enable all available encryption and privacy modes when using such services.

Where the system being used is not provided by CYC ICT you should review the platform providers privacy notice, especially around how they potentially may use voice and messaging data e.g. for marketing purposed.

Use of the Internet

Inappropriate Sites

The combination of the corporate firewall and other ICT based protection services should prevent elected members and staff from accessing or down-loading offensive, abusive or sexually explicit material and CYC will block access to certain web sites based upon the inappropriate content.

The following web content (not exhaustive) is deemed inappropriate:

- Sexually explicit, pornographic or paedophilic material
- Material which is sexist, racist, homophobic, xenophobic, or similarly discriminatory
- Offensive, derogatory or material which is liable to cause embarrassment to CYC and any of its staff or customers or bring the reputation of CYC Into disrepute
- Material advocating or encouraging illegal or violent activity
- Material in breach of copyright and/or other intellectual property rights
- Internet chat rooms
- Online gambling.

Where access to any blocked sites is required for work duties, a business case must be submitted by the relevant Head of Service to the Head of ICT. Use of these sites will be permitted for work purposes only.

Given the rate of change in Internet sites that provide access to material of this nature, and with the evolving methods of bypassing prevention, accidental access to this

material may occur. In such cases, staff must inform their manager and the ICT Service Desk immediately. Staff will not be held responsible provided that they report it immediately. If elected members access or download such material by accident, they must report it to the ICT Service Desk and as with staff, will not be held responsible provided that they report it immediately. Intentionally accessing inappropriate sites or failure to report accidental access will be treated as a serious breach of this policy.

Conditions of Use

Where access to non-essential sites is allowed i.e. Media streaming, ICT reserve the right to limit available bandwidth to prioritise and protect business critical services.

Whenever a user accesses a website, they should always comply with the terms and conditions governing its use. These rules apply at all times when using CYC issued IT equipment.

Software must not be downloaded from the Internet (to protect from viruses and copyright infringement), unless agreed in advance with ICT.

Users must comply with the conditions of copyright of any material acquired via the Internet.

Personal Use

As an enabling employer, CYC recognises that there will be occasions when elected members and staff wish to access the Internet for personal usage.

Occasional and reasonable personal use is permitted providing that:

- It is in users own time, preferably outside core hours in order to avoid unnecessary traffic on the network during peak times
- It does not interfere with the performance by elected members or staff of their duties
- It does not harm the performance of the internet system or the corporate infrastructure
- The use of the Internet conforms to all other requirements of this policy.

Examples of personal usage include:

- The booking of holidays
- Accessing auction sites like E-bay
- Obtaining traffic reports, and
- Accessing news/sporting events.

CYC are not liable for any personal security issues arising from any personal use where elected members or staff provide personal information as part of any transaction i.e. credit card details when using the internet to undertake procurement.

Abuse of CYC's Internet service is a violation of this policy. The nature of the abuse will determine the subsequent action to be taken including disciplinary proceedings.

Social Networking

Use of Social Networking Sites; Access to social media platforms (Facebook, Twitter, Flikr etc) has been provided on the understanding that people moderate any personal use.

Use Sensible Judgment

Social networking sites are publicly search-able, and almost everything posted on them is publicly accessible. If you wouldn't consider saying it face-to-face, you should reconsider putting it online.

You should exercise good judgment and take personal and professional responsibility for your online behavior.

Revealing business sensitive information about CYC in a personal online posting could be treated as gross misconduct, which may result in summary dismissal.

Remember that online participation results in your comments being permanently available and open to being re-published in other media. Stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply at all times.

Disclosing personally identifiable data about anyone, member of the public or colleague, online without there explicit consent may be a criminal offence under the General Data Protection Regulations, Data Protection Act or other UK legislation and may lead to prosecution.

Staying Safe and Secure Online

Always use a personal e-mail address as your primary means of registering for entry into social media platforms (i.e. not your CYC email address) unless they are for approved professional use.

To avoid becoming the victim of 'phishing' attacks (a fraudulent attempt, to steal personal information, such as user names, passwords or bank details) do not follow links from 'direct messages' or 'posts' on social networking sites, but type the URL into the browser bar or use a saved URL if navigating to a favourite site such as a bank or online store.

Do not click on links or advertising banners on social networking sites unless you have a good reason to trust the source. This will help to reduce the risk of intrusion from 'spyware' or 'malware' (malicious software usually embedded with a virus or destructive code).

Further details regarding the acceptable use of Social Media are available from the Head of Communications.

Instant Messaging

Instant messaging is available through Microsoft Lync. This is a business tool, all messages are recorded and all usage must conform to all other requirements of this policy.

Desktop Telephones – Personal usage

CYC recognises that there will be limited occasions when personal telephone calls need

to be made. The occasional and reasonable use of the telephone for personal calls using a personal telephone charge card (not supplied by CYC) that will then be used by the employee to record and ensure that the associated call costs are charged to the card is acceptable only if the calls are undertaken in the user's own time and it does not

interfere with the performance of work duties. This does not relate to calls which are urgent and directly business related and necessary for employees' peace of mind e.g. to phone home or make child care arrangements when working late, if notice was given that day. All calls made are logged in terms of duration and number dialled and the relevant departmental budget holders can request a breakdown of calls (this service may incur a charge) made by extension number if required to verify the presence of non business calls made.

Persistent abuse of desktop phones that interrupt the effectiveness of staff productivity or bring CYC into disrepute will result in action being taken in accordance with CYC's disciplinary procedures.

Examples of abuse include:

- Making personal/non business related calls without using a personal telephone card;
- Making excessive numbers of personal calls during recorded working hours; and
- Making threatening or abusive phone calls.

Use of CYC Mobile phones / Smartphones

Mobile phones are provided following an approved and authorised business request and are issued on the understanding that they are for business use.

CYC recognises that there will be occasions when staff with CYC supplied mobile phones may need to use them for personal calls. These calls must be made in a users own time.

In order that staff can be recharged for their personal calls, mobile users should, after keying in their required number:

- Press the * key three times *** and then the **Enter** or **Send** key.

- The phone account, when produced for authorization, will then have the *** symbol showing against personal call costs.

- Staff must ensure that all personal calls are made using the *** key process and reimburse CYC for these costs via their line manager.

As with desktop telephones, personal calls which are urgent and business related and necessary for employees peace of mind e.g. to phone home or make child care arrangements when working late, fall outside these arrangements and do not require the use of the *** key to identify them as personal calls.

Tracking Electronic Communications Usage

The use of all means of electronic and telecommunications services including telephone, email, the Internet and Social Media activity is subject to tracking in accordance with this policy in order to detect and deal with abuse of the system. In using any of these services for private use, all users are consenting to reasonable tracking of such private use being carried out in accordance with this policy where there are reasonable grounds to suspect misuse or abuse of services.

As part of preventing any misuse or abuse, all line managers are responsible for making themselves and their staff aware of this electronic communications policy and the

potential for instigating disciplinary action where misuse is suspected and subsequently proven.

If a line manager suspects misuse or abuse, they should contact the ICT Service Desk immediately who will supply a "User Investigation request form". This requires sign off by the relevant directorate Director or nominated deputy and the Head of ICT before details of usage are made available through the monitoring facilities detailed below.

Any proven misuse or abuse will be managed and enforced through CYC's disciplinary procedure.

CYC's ICT department have monitoring facilities that allow for continuous or ad-hoc tracking of usage of Internet, telephone and email (internal and external) services. This could lead to an investigation if misuse was discovered through the passive non-invasive monitoring, during fault resolution duties or as directed by an authorised User Investigation Request Form using the agreed formal procedure as outlined above.

These facilities are principally designed to allow ICT to optimise the value of CYC's investment in information technology and ensure its continual good reputation through:

- Continually monitoring network and system performance, throughput, response times and usage;
- Ensuring the network is set-up and maintained to give optimum usage and performance;
- Remote fault diagnosis and fault resolution ('shadowing'); and
- System training.

However, these facilities can be deployed to track the use of electronic communications where there are reasonable grounds to suspect misuse or abuse and an approved investigation is taking place. Shadowing for remote fault diagnosis and resolution can only take place with a user's permission.

Users should not have any expectation of total 'privacy' in relation to accessing websites, personal email correspondence or personal documents stored on CYC's corporate file storage system or messages sent via the Internet. In principle, these may be subject to the same checking procedures applied to business related access and email correspondence.

Monitoring is, however, only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Enforcement

Staff

This policy, and subsequently proven breaches, will be enforced and managed by CYC's agreed and approved disciplinary procedures.

The level of action taken in response to inappropriate or misuse will be dependant on the nature of the misuse and the subsequent risks to the Council's reputation and infrastructure.

CYC considers serious abuse (see below) of the policy to constitute gross misconduct and minor abuse to constitute misconduct. Allegations of misuse will be investigated and

action taken in accordance with CYC's disciplinary procedure. Without prejudice to the process, gross misconduct will result in dismissal without notice if proven at the disciplinary hearing.

Any suspected breaches of this policy are to be managed by the local line manager with assistance from ICT and Human Resources and in accordance with CYC's disciplinary procedures.

Below are examples of the types of offence that constitute gross misconduct or misconduct. These lists are not exhaustive and there may be other offences that will result in disciplinary action being taken. Every offence will be carefully considered, and disciplinary action will be taken in accordance with the disciplinary procedure depending on the seriousness of the case and in the light of all the circumstances.

Certain offences that normally constitute gross misconduct may constitute misconduct only because of mitigating circumstances. Similarly, certain issues normally viewed as misconduct, could, due to the serious nature of the offence, constitute gross misconduct.

Elected Members

The Director of Customer and Corporate Services in conjunction with the Head of ICT will manage abuse of this policy by undertaking a documented review with the elected member involved. The review will be recorded and the documents will be retained within the centrally held register. The outcome of such a review will be reported to the Group Leader and Whip of any member who belongs to a political group.

A failure to comply with this policy is likely to be a breach of a Member's obligation under the Council's code of conduct to abide by the council's reasonable requirements when using the resources of the Council. Serious or repeated breaches of the policy may result in a referral to the Council's Standards Committee.

Third Parties

Any abuse or suspected abuse will be reported to the senior representative of such third party. CYC reserve the right to suspend or terminate services provided dependant on the circumstances and related risk to the council and its ICT infrastructure

Examples of minor abuse include:

Email

- The inappropriate sending of messages; including unsolicited mailings to a large number of users (spamming).
- Burdening the e-mail system with non-business data especially the transmission of large data files and/or large attachments to one or a number of recipients.
- Originating or participating in e-mail chain letters.
- The use of explicit, obscene or profane language in e-mail communication with colleagues.
- The substantial personal use of e-mail involving the external transmission of large documents, adding an unnecessary burden to the corporate e-mail system and corporate network.

Internet

- Persistent low volume personal usage during core hours
- Failure to comply with the notification process as defined within this policy.

Examples of serious abuse include:

Email

- The creation, sending or forwarding of material that is offensive, discriminatory, abusive, libellous or illegal, including, but not limited to, material of a racist, sexist, homophobic, sexually explicit or discriminatory nature
- Intentionally generating any messages containing sexual, discriminatory, offensive or illegal material
- Intentionally forwarding messages with known viruses that could threaten the availability and integrity of the Council's infrastructure or information.
- Deliberately using e-mail in such a way that it constitutes harassment or bullying
- Forwarding sensitive Council information or personal data to unapproved external sources
- Maliciously modifying a message and forwarding it without highlighting the changes, or deleting the original author's name

General

- Repeated minor abuses of the policy

Termination of Employment

When a user who has network access leaves the employment of the Council the appropriate manager must arrange for the transfer of any necessary files and e-mail folders.

Where termination is due to ongoing disciplinary action the user's access will be denied with immediate effect.

The appropriate Line Manager must notify ICT, using the relevant online form Delete user request, that the user is leaving so that the user's login credentials can be removed from the network. This removal will not take place earlier than 28 days after the user has left to allow for the deletion or transfer of files, data and emails within the department. However the user's access rights will be disabled immediately.

On termination it is the user's responsibility to return all equipment, entry passes, software, documentation (both paper and electronic) and any other Council asset in their possession.