ARMAGH BANBRIDGE CRAIGAVON DISTRICT COUNCIL	
Document Reference Number:	**GRSC/P5.0/V1.0**
Title of Policy:	**ICT Acceptable Use Policy**
No of Pages (including appendices):	
Version:	
Issue Date:	
Policy Nominated Officer:	**Conleth Donnelly ICT Services Manager**
Equality screened/Rural Impact Assessment:	**Conleth Donnelly ICT Services Manager**
Equality screening/Rural Needs Impact Assessment date:	**02. 09. 19**
Amendment Version Issue Date:	
Sent out by:	
Approved by:	
Review Date:	

AMENDMENT RECORD SHEET

Remove and destroy old pages. Insert new pages as indicated.

Revision Number	Page Number	Date Revised	Description of Revision

1. INTRODUCTION

Armagh City, Banbridge and Craigavon Borough Council Information and Communications Technology (ICT) systems, services and facilities are provided to enable employees and other authorised individuals to perform their roles effectively and efficiently.

2. PURPOSE

The purpose of this policy is to identify proper usage and behaviour when using Council ICT systems. The policy is designed with the overall aim of protecting the integrity of the ICT resources, information systems and data. The policy also aims to ensure that all users of the Council ICT are clear about what is acceptable and unacceptable ICT usage.

3. SCOPE

This policy applies to all Council employees, persons representing the Council (including sub-contractors and consultants), Trade Union representatives and Elected Members using Council ICT resources.

The term ICT includes all computing devices (including mobile devices such as Tablets and smart phones), printers, photocopiers and multifunctional devices that are owned, operated or managed by the council. It also refers to Information Systems and services, all software, networks, internet access and email systems owned or operated by the council.

This policy applies to all aspects of ICT use, whether undertaken in a Council location or elsewhere.

Those to whom this policy applies must only use ICT equipment or services that has been authorised for their use. Any attempt to gain unauthorised access to any system provided by Council or to use Council ICT resources to gain unauthorised access to any other system is a breach of this policy and may also be a breach of legislation (including the Computer Misuse Act 1990).

4. POLICY DETAIL

4.1 Acceptable Use of ICT Equipment and Services

The effective operation of Council ICT systems relies heavily on the proper conduct of the users.

The use of all ICT facilities must follow all appropriate legislation, relevant codes of conduct and Council Policies and guidance.

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

in support of business and service needs consistent with Council policies;

in support of an individual's job role and responsibilities wihin Council;

be consistent with any other Council policies, procedures and guidance appropriate to the system, network or service being used or accessed

4.2 Unacceptable Use of ICT Equipment and Services

It is unacceptable for anyone to use Council ICT systems or devices to carry out any activity which:

- puts the integrity of Council systems or information at risk;
- violates or infringes upon the rights of any other person, including the right to privacy;
- is contrary to any Council Policies;
- is detrimental to the reputation of the Council;
- contains defamatory, abusive, obscene, pornographic, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material;
- encourages the use of controlled substances or illegal behaviour;

- uses the system for any illegal purpose;
- breaches legislation or statutory requirements with which the Council must comply e.g. GDPR or Copyright Designs & Patents Act 1988.

It is not acceptable for a user to use the facilities and capabilities of the ICT systems to:

- conduct any non-approved business;
- download or install any unauthorised or unlicensed software;
- 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 or 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;
- 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 Council filtering or monitoring functions, any safety measures, controls or configuration applied by the ICT Service;

Council ICT equipment, including tablets and smart phones, is issued to employees and other authorised individuals to perform their roles effectively and efficiently. Access to any Council ICT equipment should not be shared with any individual outside of the organisation. It is the responsibility of employees and other authorised individuals to take appropriate care to protect any equipment, or access rights that have been issued to them.

4.3 Acceptable use of Council Email System

- All use of email must be consistent with Council's acceptable use of ICT Equipment and Services (Section 4.1 and 4.2 above)
- By default, email is not encrypted. Users should consider email an unsecure form of communication. Risks exist when transmitting any proprietary, confidential, or otherwise sensitive information over the Internet. Users should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Consideration should be given to the sensitivity of the information being transferred and the transmission process. Adequate controls and safeguards should be applied for example password protection and encryption of attachments. Users should also be aware that once an email is transmitted it may be altered. Deleting an email from an individual workstation will not eliminate it from the various systems across which it has been transmitted.
- Users are prohibited from inappropriately forwarding Council emails to any third party including a private email. Individual messages which are forwarded by the user must not contain Armagh City, Banbridge and Craigavon Borough Council confidential information.
- Users are prohibited from using third-party email systems and data storage services such as Google, Yahoo, Dropbox and MSN Hotmail etc. to conduct Council business, to create or memorialize any binding transactions, or to store or retain email on behalf of Council. Such communications and transactions should be conducted

through proper channels using Council approved documentation. Council business should only be conducted using Council email accounts and services.
- Sending chain letters or joke emails from a Council email account is prohibited.
- Council employees shall have no expectation of privacy in anything they store, send or receive on the Council email system.
- All emails circulating within the Council email system are archived. This archive is searchable.
- Reports on usage can be produced as required.
- Emails are a Council record and may be subject to Information requests under Freedom of Information legislation

4.4 Acceptable Use of Council Provided Internet Access

- All use of internet access must be consistent with Council's acceptable use of ICT Equipment and Services (Section 4.1 above)
- Internet usage is granted for the purpose of supporting business activities necessary to carry out job functions.
- Limited personal use is permitted e.g. during lunchtime, in so far as it does not interfere with service delivery and is in the user's own time. Users of this service should be aware activity is monitored and a log is retained. Staff using the Council internet service for personal activity do so at their own risk. The council is not responsible for any loss of information, or any consequential loss of personal property when using Council internet services for personal use.
- Acquisition, storage, and dissemination of content which is illegal, pornographic, or which negatively depicts any individual or group is specifically prohibited.
- Council prohibits the conduct of a business enterprise, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.
- Council also prohibits any form of gambling using the Council Internet access
- Risks exist when transmitting any proprietary, confidential, or otherwise sensitive information over the Internet. Consideration should be given to the sensitivity of the information being transferred and the transmission process. Adequate controls and safeguards should be applied for example password protection and encryption.
- Bandwidth both within Council and when connecting to the Internet is a shared, finite resource. This is particularly the case in smaller sites which have smaller bandwidth connections Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees.
- Users should be aware that Internet activity is automatically logged and can be reported upon at the request of line managers. This examination ensures compliance with internal policies and assists with the management of Council information systems.
- Internet access information is a record of the organisation and may be subject to Freedom of Information legislation

4.5 Passwords and Security

Passwords and/or pass codes are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of Council information or resources. All users, including partners, contractors and software suppliers with access to Council systems, are responsible for taking the appropriate steps, as outlined below, to protect and secure their accounts and passwords.

- All user-level and system-level passwords must conform to the Password Construction Guidelines which are available on the ICT Helpdesk Portal.

- The same password should not be repeated or used for multiple accounts.
- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, confidential Council information.
- No one should ever request another person's password under any circumstances.
- Passwords must never be inserted into email messages, or any form of electronic communication.
- Passwords should never be written down or stored anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Any user suspecting that his/her password may have been compromised must report the incident immediately to the ICT Helpdesk.
- Council passwords should never be shared with anyone, including administrative assistants, secretaries, managers, co-workers, or family members.

Users must:

- not use or attempt to use another individual's account or password;
- 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 ICT immediately if they suspect or identify a security problem or a breach of the Acceptable Use of ICT Policy by any user;
- contact ICT immediately if any equipment is lost or stolen.
- take all reasonable precautions to protect Council ICT data, information systems and resources and from security issues such as computer viruses and malware.
- use only properly supplied and authorised systems for undertaking Council business only;

*4.*5 USB storage devices

- Use of USB storage is restricted
- Only Council issued encrypted USB Storage devices should be used to store Council information and Council information only.
- Only Council USB storage devices should be connected to Council equipment.

5. RELATED POLICIES

6. EQUALITY SCREENING FORM (to be attached as an appendix to all policies)

7. DRAFT EQUALITY IMPACT ASSESSMENT AND OTHER IMPACT ASSESSMENTS

EQIA deemed unnecessary.

Policy Screening Form

Policy Scoping

Policy Title: ICT Acceptable Use Policy

Brief Description of Policy (please attach copy if available). Please state if it is a new, existing or amended policy.

The purpose of this policy is to identify proper usage and behaviour when using Council's ICT systems. This is a new policy for Armagh City , Banbridge and Craigavon Borough Council though policies existed in previous organisations

Intended aims/outcomes. What is the policy trying to achieve?

The policy is designed with the overall aim of protecting the integrity of the ICT resources, information systems and data. The policy also aims to ensure that all users of the Council's ICT are clear about what is acceptable and unacceptable ICT usage.

Policy Framework

Has the policy been developed in response to statutory requirements, legal advice or on the basis of any other professional advice? Does this affect the discretion available to Council to amend the policy?

Professional Advice in internal and External Audit. No this does not affect the discretion of the council to amend the policy

Are any Section 75 categories which might be expected to benefit from the policy? If so, please outline.

The policy is intended to benefit all employees regardless of equality group they fall within.

Who initiated or wrote the policy (if Council decision, please state). Who is responsible for implementing the policy?

Who initiated or wrote policy? ICT Service Manager	**Who is responsible for implementation?** ICT Service Manager

Are there any factors which might contribute to or detract from the implementation of the policy (e.g. financial, legislative, other)?

No

Main stakeholders in relation to the policy
Please list main stakeholders affected by the policy (e.g. staff, service users, other statutory bodies, community or voluntary sector, private sector)

This policy applies to all Council employees, agents of the Council, persons representing the Council (including sub-contractors and consultants), Trade Union representatives and elected members using Council ICT resources.

Are there any other policies with a bearing on this policy? If so, please identify them and how they impact on this policy.

Social Media Usage Policy
Code of Conduct
Data Protection Policy

Available Evidence

Council should ensure that its screening decisions are informed by relevant data. What evidence/information (both qualitative and quantitative) have you gathered to inform this policy? Specify details for each of the Section 75 categories.

Section 75 category	**Evidence**
Religious belief	N/A
Political opinion	N/A
Racial group	N/A
Age	N/A
Marital status	N/A
Sexual orientation	N/A
Men and women generally	N/A
Disability	N/A
Dependants	N/A

Needs, experiences and priorities

Taking into account the information gathered above, what are the different needs, experiences and priorities of each of the following categories in relation to this particular policy/decision?

Section 75 category	**Needs, experiences and priorities**
Religious belief	N/A
Political opinion	N/A
Racial group	N/A
Age	N/A
Marital status	N/A
Sexual orientation	N/A
Men and women generally	N/A
Disability	N/A
Dependants	N/A

Screening Questions

1. What is the likely impact on equality of opportunity for those affected by this policy for each of the Section 75 categories?

Category	Policy Impact	Level of impact (Major/minor/none)
Religious belief	N/A	
Political opinion	N/A	
Racial group	N/A	
Age	N/A	
Marital status	N/A	
Sexual orientation	N/A	
Men and women generally	N/A	
Disability	N/A	
Dependents	N/A	

2. Are there opportunities to better promote equality of opportunity for people within the Section 75 categories?

Category	If yes, provide details	If no, provide reasons
Religious belief	N/A	
Political opinion	N/A	
Racial group	N/A	
Age	N/A	
Marital status	N/A	
Sexual orientation	N/A	
Men and women generally	N/A	
Disability	N/A	
Dependents	N/A	

3. To what extent is the policy likely to impact on good relations between people of different religious belief, political opinion, or racial group?

Category	Details of Policy Impact	Level of impact (major/minor/none)
Religious belief	N/A	
Political opinion	N/A	
Racial group	N/A	

<table>
<tr><td colspan="3"><b>4. Are there opportunities to better promote good relations between people of different religious belief, political opinion or racial group?</b></td></tr>
<tr><td>Category</td><td>If yes, provide details</td><td>If no, provide reasons</td></tr>
<tr><td>Religious belief</td><td>N/A</td><td></td></tr>
<tr><td>Political opinion</td><td>N/A</td><td></td></tr>
<tr><td>Racial group</td><td>N/A</td><td></td></tr>
</table>

Multiple Identity

Generally speaking, people fall into more than one Section 75 category (for example: disabled minority ethnic people; disabled women; young Protestant men; young lesbian, gay and bisexual people). Provide details of data on the impact of the policy on people with multiple identities. Specify relevant s75 categories concerned.

N/A

Disability Discrimination (NI) Order 2006

Is there an opportunity for the policy to promote positive attitudes towards disabled people?

N/A

Is there an opportunity for the policy to encourage participation by disabled people in public life?

N/A

Screening Decision

A: NO IMPACT IDENTIFIED ON ANY CATEGORY – EQIA UNNECESSARY

Please identify reasons for this below

This is a technical policy, the purpose of which is to outline the acceptable use of computer equipment at Armagh City, Banbridge and Craigavon Borough Council. It has no bearing in terms of its likely impact on equality of opportunity or good relations categories.

B: MINOR IMPACT IDENTIFIED – EQIA NOT CONSIDERED NECESSARY AS IMPACT CAN BE ELIMINATED OR MITIGATED

Where the impact is likely to be minor, you should consider if the policy can be mitigated or an alternative policy introduced. If so, EQIA may not be considered necessary. You must indicate the reasons for this decision below, together with details of measures to mitigate the adverse impact or the alternative policy proposed.

C: MAJOR IMPACT IDENTIFIED – EQIA REQUIRED

If the decision is to conduct an equality impact assessment, please provide details of the reasons.

Timetabling and Prioritising

If the policy has been screened in for equality impact assessment, please answer the following questions to determine its priority for timetabling the equality impact assessment.

On a scale of 1-3 with 1 being the lowest priority and 3 being the highest, assess the policy in terms of its priority for equality impact assessment.

Priority criterion	**Rating (1-3)**
Effect on equality of opportunity and good relations	1
Social need	1
Effect on people’s daily lives	1

The total rating score should be used to prioritise the policy in rank order with other policies screened in for equality impact assessment. This list of priorities will assist the council in timetabling its EQIAs.

Is the policy affected by timetables established by other relevant public authorities? If yes, please give details.

N/A

Monitoring

Effective monitoring will help the authority identify any future adverse impact arising from the policy. It is recommended that where a policy has been amended or an alternative policy introduced to mitigate adverse impact, monitoring be undertaken on a broader basis to identify any impact (positive or adverse).

Further information on monitoring is available in the Equality Commission's guidance on monitoring

Identify how the impact of the policy is to be monitored

The Policy will be reviewed annually.
There is a feedback form in the ICT portal and there will be annual meetings with HOD regarding all range of ICT services. The ICT Policy will be discussed then with HsOD at the regular meeting along with any other current or future ICT policies.

Approval and Authorisation

A copy of the screening form for each policy screened should be signed off by the senior manager responsible for that policy. The screening recommendation should be reported to the relevant Committee/Council when the policy is submitted for approval.

Screened by	Position/Job title	Date
Conleth Donnelly	ICT Services Manager	
Approved by	Position/Job Title	Date
Sharon McNicholl	Strategic Director – Performance	

Please forward a copy of the completed form with policy attached to mary.hanna@armaghbanbridgecraigavon.gov.uk who will ensure that screening forms and policies are available on the Council website.

This officer is also responsible for issuing reports on a quarterly basis on those policies "screened out for EQIA". This allows stakeholders who disagree with this recommendation to submit their views. In the event of any stakeholder disagreeing with the decision to screen out any policy, the screening exercise will be reviewed.