East Dunbartonshire Council

Acceptable Use Policy for East Dunbartonshire Council's ICT Facilities

Overview:

This policy sets out the authorised use of East Dunbartonshire Council's ICT Facilities by employees, Elected Members, pupils and members of the public.

Failure to comply with this policy could result in access to ICT facilities being suspended or withdrawn completely.

Employees may also face disciplinary action.

Section 1	Relates to employees and Elected Members use of Council ICT facilities
Section 2	Relates to members of the public using ICT in Council Buildings such as libraries and community centres
Section 3	Relates to pupils using Council computers in Schools
Section 4	Use of the Internet by Young Children in Early Years Settings
Section 5	Contains a Parent / Carer's Guide to the Safe Use of Internet and Email

East Dunbartonshire Council

TABLE OF CONTENTS

East Dunbartonshire Council

Document Control

Owner:	Peter English Information Security Manager East Dunbartonshire Council
Source Location:	H:\PUBLIC\BC&IS\01. Information Security\01.99 ISMS\Acceptable use of ICT Facilities Policy v1.4.doc
Document Reference:	TBA
Other Documents Referenced:	Access Control Policy Child Protection Policy Contract of Employment Covert Monitoring Policy Home Working Policy Incident Investigation Policy Information Classification and Protection Policy Mobile Phone Policy
Related Documents:	
Acknowledgements:	Information Security Board

This document is subject to change control and any amendments will be recorded below.

Change History

Version	Date	Circulation	Changes	Author
0.8	08 January 2008	Information Security Improvement Board	Document control table added Modifications and additions highlighted in red to the following paragraphs: 2.1.4 3 3.3.9 Deletions 7.1.6 Appendix A	PE
0.9	05 February 2008		Amended to reflect comments of IS Board and Allan Lauder. 5.3.2., 5.4.1., 6.1.3., 11.1.4 , 14.2	PE
0.10	17 February 2008		Details relating to personal use of web-based email changed. Minor changes for readability and typos.	PE
1.0	03/03/03	CMT		PE
1.1	14/05/08		Typos	PE
1.2	12/06/08	Trainers	Formatting + Comment Added	PE
1.3	19/06/08	Trainers	Compliance Statement	PE
1.4	29/08/08	P&R	Jim Corrigan's comments added to signature for pupils over 16 . p.46	PE
2.0	25/09/08	Approved by P&R	None	PE

Version Awareness
This document may not be the latest available version. The latest version, which supersedes all previous versions, is available at: <LINK to Hub Page>

East Dunbartonshire Council

1 SECTION 1: Acceptable Use Policy for Employees and Elected Members Using East Dunbartonshire Council's ICT Facilities

Purpose:

This policy sets out the authorised use of:

- All electronic equipment capable of information processing;
- All peripherals such as scanners, printers and photocopiers;
- All software including, but not restricted to, Internet browsers and email;
- All cabling and sockets;
- All other Council communication facilities such as telephones, mobile telephones and answer-phones and faxes.

Contacts

Information Security Manager	0141 574 5560
information.security@eastdunbarton.gov.uk	
ICT Service Desk (General ICT related issues)	0141 578 8888
Freedom of Information & Data Protection Officer	0141 775 4571
Admin Coordinator (Mobile phone enquiries)	0141 574 5623

2 Compliance with Information Security Policies

2.1.1 Failure to comply with the Acceptable Use Policy, Mobile Devices Policy and Information Classification and Protection Policies may result in disciplinary action being taken under the Council's disciplinary procedures the consequences of which can include dismissal, or the withdrawal of permission to use the Council's ICT equipment for personal purposes. If there is anything in this policy that you do not understand, please discuss it with your line manager.

2.1.2 Please note that the procedures and policies outlined in this policy, and in any related policy, may be reviewed or changed at any time. You will be alerted to important changes, and updates will be published on the Council's intranet.

2.1.3 You must sign this page to indicate that you understand, and will abide by, the contents of the Council's Information Security Policies.

2.1.4 I agree to:

- Comply with the terms of the Acceptable Use Policy, Mobile Devices Policy and Information Classification and Protection Policy;
- Take all reasonable steps to safeguard the business equipment and information of the Council;
- Ensure that my use of Council ICT facilities is limited, reasonable, responsible and not excessive, as defined in the Acceptable Use Policy;
- Only use Council equipment and / or access the Corporate network for the purposes which I have been authorised;
- Not view or distribute racist, sexist, pornographic material or any material which seeks to encourage religious hatred;
- Not to use email, the internet or any other software to insult, bully, harass or defame;
- Not infringe copyright or intellectual property laws, including downloading files which it is illegal / a breach of copyright to use;
- Not remove or subvert security measures or otherwise making unauthorised changes to equipment or software, or allowing others to do so;
- Not knowingly distribute viruses, or any form of malware (any software or code with malicious intent);
- Not to install any software without authorisation from ICT Services;
- Respect people's privacy and confidentiality and comply with the Data Protection Act 1998;
- Safeguard my passwords and not share them;
- Not to allow unauthorised third-parties (e.g. children or friends) to use EDC equipment;
- Log out or lock my computer if I leave my workstation unattended (to do this press ctrl-alt-del and select 'lock workstation'); and
- Ensure that regular rest breaks are taken;

Name:	
Service/Department	
Signature:	
Date:	

Policy edition: Tuesday, 22 July 2025

3 Introduction

East Dunbartonshire Council's (The Council's) information and communications facilities are provided by Information and Communications Technology Services (ICT) and made available to users for the purposes of the Council's business. A certain amount of limited, reasonable and responsible personal use is permitted.

- Limited – means limited to business use and, where permitted, personal use subject to the discretion of line managers and the constraints set in this policy. Personal use should only take place outwith your working hours – i.e. before and after you begin work or in lunch or other official breaks.
- Reasonable – means that personal usage of Council ICT facilities must not interfere with the performance of work duties and must not impede the operation of East Dunbartonshire Council ICT facilities or Services.
- Responsible – means that users must be cognisant of the contents of this policy and other applicable Council policies, which set out the rights and responsibilities of employees or Elected Members of East Dunbartonshire Council.
- Excessive use - is usage which interferes with the performance of employees' or Elected Members' duties to the Council.

East Dunbartonshire Council is committed to the utilisation of advances in Information and Communications Technology. Information and communication plays an essential role in the conduct of the Council's business. Corporate communications not only reflect on individuals but also on the Council as an organisation. The Council values the capacity that ICT gives employees and Elected Members to communicate with colleagues, members of the public and work contacts, and the Council invests substantially in information technology and communications systems which enable you to work more efficiently. The Council trusts employees and Elected Members to use ICT responsibly.

Anybody seen misusing the system or any inappropriate material encountered should be reported to the appropriate line manager.

3.1 Scope

This policy applies to all employees and Elected Members of East Dunbartonshire Council who use the Council's ICT facilities. 'employees' refers to all personnel whether they are full-time, part-time or fixed-term employees, trainees, tutors, volunteers, contractors, temporary employees or home-workers.

ICT facilities refer to equipment and / or systems which include:

- Desktop PCs
- Laptops
- PDAs (Personal Digital Assistants)
- Printers
- Servers
- Email
- Intranet
- Internet
- Miscellaneous Software
- USB sticks and other peripherals and devices
- Digital or still cameras
- Photocopiers and scanners
- Telephones and telephone equipment
- Answer-phones / voicemail
- Faxes

All use of the Council's ICT facilities is governed by the terms of this policy. If the Council's rules and procedures are not adhered to, then use of ICT facilities may be curtailed or withdrawn and disciplinary action may follow. In accordance with the Council's Disciplinary Procedures, serious breaches of this policy may be treated as gross misconduct which can result in dismissal.

Teaching and Education Services Support Staff must abide by this policy whilst using equipment outwith the Council to access the National Educational Portal (GLOW).

Although the detailed discussion of this policy is limited to use of computing equipment, email and Internet facilities, telephone communications and fax machines, the general principles underlying all parts of this policy also apply to all software, printers, copiers and scanners.

Please contact the Information Security Manager with any questions.

3.2 Legal Precedence

For the avoidance of doubt, and in the event of an apparent contradiction occurring between legislation, policy or best practice guidelines, legislation will take priority. This also applies to any future legislation that may be enacted.

3.3 General Principles

3.3.1 Employees and Elected Members must use the Council's ICT facilities sensibly, professionally, lawfully, in a manner consistent with their duties, with respect for their colleagues and the Council, in accordance with this policy and the Council's other rules and procedures.

3.3.2 The Council permits limited personal use of ICT facilities provided that personal use:

- Takes place outwith working hours i.e. before or after work or during lunch or other breaks;
- Does not interfere with the performance of Council duties;
- Does not take priority over work responsibilities;
- Does not cause unwarranted expense or any liability to be incurred by the Council;
- Does not have a negative impact on the Council in any way; and
- Is lawful and complies with this policy.

3.3.3 Employees and Elected Members must treat the Council's paper-based and electronic information with the utmost care. Individuals can request information held about themselves under the Data Protection Act 1998 and business and individuals can request a very wide range of information under the Freedom of Information Scotland Act 2002. In all such cases, this could include information contained in emails and other communications by Council employees. Communications, even internal communications, should be made with the assumption that they will be disclosed.

3.3.4 Particular care must be taken when using email, the intranet or internal message boards as a means of communication because all expressions of fact, intention and opinion may be binding on individuals and / or the Council and can be produced in court in the same way as other kinds of written statements.

3.3.5 The advantage of the Internet and email is that they are extremely easy and informal ways of accessing and disseminating information, but this means that it is also easy to send out ill-considered statements. Employees and Elected Members should ensure that messages sent on email systems or over the Internet display the same professionalism they would apply when writing a letter or a fax. Employees and Elected Members must not use these electronic media to do or say anything which would be subject to disciplinary or legal action in any other context, such as sending any discriminatory (on the grounds of a person's sex, race, age, sexual orientation, religion or belief), defamatory or other unlawful material. Employees should take advice

from their line manager or the Information Security Manager if they have any queries regarding this aspect of the policy.

3.3.6 Many aspects of communication are protected by intellectual property rights, which can be infringed by downloading, uploading, posting, copying, possessing, processing and distributing material. Employees and Elected Members should only use material in a manner consistent with copyright and intellectual property rights.

3.3.7 Employees and Elected Members using the Council's systems to access the internet do so at their own risk. The Council will not be responsible for losses incurred by Elected Members or employees while making use of the Internet or email services for personal transactions.

3.3.8 The Council reserves the right to monitor and log all aspects of its computer systems and networks, including Internet sites visited by users, information exchanged with Internet sites and the downloading of files of all types.

3.3.9 The content of email communications sent and received by users is automatically filtered and content may be accessed to resolve technical problems or where there is reasonable suspicion of a breach of the Policy. The Council reserves the right to access employees email where there is a legitimate business need to do so, for example, to ensure business continuity when employees are absent from work for lengthy periods.

3.3.10 The Council reserves the right to monitor all network activity without notice, to facilitate maintenance, improvements to the service, or where there is reasonable suspicion of a breach of this Policy. Therefore users can have no expectation of privacy while making use of any Council ICT facilities.

3.4 Responsibilities

3.4.1 All Employees and Elected Members

Employees and Elected Members are responsible for the following:

- Complying with the terms of this policy;
- Taking all reasonable steps to safeguard the business equipment and information of the Council;
- Only using Council equipment or accessing the Corporate network for authorised purposes;
- Not viewing or distributing racist, sexist, pornographic or any material which seeks to encourage racial hatred;
- Not infringing copyright or intellectual property laws, including downloading files which it is illegal / a breach of copyright to use;
- Respecting people's privacy and confidentiality and complying with the Data Protection Act 1998;
- Safeguarding passwords – i.e. not writing them down or sharing them with colleagues;
- Reporting anyone who they believe to be using systems inappropriately to the relevant manager (who should report the incident to the Information Security Manager);
- Not removing or subverting security measures or otherwise making unauthorised changes to equipment or software or allowing others to do so;
- Not knowingly distributing viruses, or any form of malware (any software or code with malicious intent);
- Not installing any software without authorisation from ICT Services;
- Not allowing unauthorised third-parties (e.g. children or friends) to use EDC equipment;
- Logging out or locking computers if their workstation is left unattended i.e.: when moving away from their PC (press ctrl-alt-del and select 'lock workstation');
- Not using email, the internet or any other software to insult, bully, harass or defame; and
- Ensuring workstations comply with health and safety requirements and that regular rest breaks are taken.

3.4.2 Employees supervising third-party use of the Internet

Employees facilitating public or school children's use of ICT facilities are responsible for the following:

- Ensuring that they have read and comply with the Council's child protection policies;
- Ensuring that all users, or their parents, carers and /or guardians understand, and have signed to indicate that they understand, the Acceptable Use Policy;
- Ensuring that they are aware of the procedures for reporting misuse and ensuring that they notify the Information Security Manager; and
- Ensuring that best endeavours are made to offer protection from material which may be deemed unsuitable to users of the Council's Internet and email services.

3.4.3 Line Managers' responsibilities

Line managers are responsible for ensuring that their employees abide by the above, and in addition:

- For ensuring that all users who report to them have signed to indicate that they understand and will abide by, the Acceptable Use Policy;
- For managing and reporting any inappropriate use in accordance with the Breach of Acceptable Use Procedure Breach of Acceptable Use Procedure;
- For assessing and addressing training requirements promptly so individuals can use systems effectively; and
- For ensuring that workstation assessments are carried out by the Council's Health and Safety function.

3.4.4 Authorised Equipment

Only equipment authorised by ICT should be attached to the Council's Network. ICT Service Desk will be able to confirm whether equipment is authorised. Personal USB devices should not be attached to Council ICT facilities without prior authorisation.

4 Use of Telephone and Fax Equipment

4.1 General

4.1.1 Telephone and fax equipment is provided to employees and Elected Members for the Council's business purposes.

4.1.2 The Council receives telephone and / or fax bills for each Section, containing the numbers dialled, the length of calls and the cost of those calls. It is the responsibility of line managers to ensure that their employees do not misuse telecommunications equipment.

4.1.3 The Council does not normally intercept calls but in certain rare circumstances, where there are reasonable grounds to suspect serious misconduct and, subject to compliance with applicable legislation, the Council reserves the right to record calls (see the Council's Covert Monitoring Policy for further details).

4.2 Personal Use

4.2.1 The Council recognises that there will be occasions when employees and Elected Members need to make short, personal calls on Council telephones, both fixed lines and mobiles, in order to deal with occasional and / or urgent domestic crises. Routine personal calls should be made using a personal mobile telephone. Non-urgent calls should be made during scheduled breaks or outside of the normal working day when they do not interfere with work requirements.

4.2.2 Equally, it is legitimate to receive personal calls about domestic crises and arrangements, and occasional, short, non-urgent calls can be received providing they do not interfere adversely with work requirements.

4.3 Calls to Mobile Telephones

4.3.1 Calls to mobile telephones are particularly expensive and these should be kept to an absolute minimum whether for business or personal purposes.

4.3.2 Calls between Council mobile phones are cheaper than a call from a Council landline to a Council mobile. Therefore, where practicable, employees should choose the cheaper option and phone other council mobile phones using their corporate mobile.

4.4 118 Numbers

4.4.1 Employees and Elected Members should not call 118 numbers unless the free alternatives to the service list below are unavailable. Calls to 118 numbers represent a significant cost to the Council. Free phone directory information is available from the following sources:

- www.thephonebook.bt.com
- http://www.yell.com

4.4.2 Calls to 118 from a desk phone should be directed to the Council's preferred 118 provider: **118707**. Employees must not ask to be put through to their destination as this costs a significant amount of money instead they must take a note of the number and then call it.

4.4.3 Calls from mobile phones should be directed to 118888, who are Vodafone's preferred provider.

4.5 Premium rate and international calls

4.5.1 Employees should not make calls or send faxes to international or premium-rate numbers, for any purpose without the prior permission of their line manager. International numbers start '00' and premium rate numbers begin '09'.

4.5.2 The use of Council telephones, for either private or Council purposes, which are in any way excessive (i.e. outside of the limits defined above), defamatory, obscene or otherwise inappropriate, could be treated as misconduct under the Council's disciplinary procedure. In serious cases this could be regarded as gross misconduct.

5 Use of Council Mobile Telephones

5.1 General

5.1.1 Employees who require a mobile device to perform work duties should request authorisation from their line manager.

5.1.2 Devices supplied by the Council must only be used by the designated user. Employees must be aware of their responsibilities under this Policy, the Council's mobile phone policy and cognisant of the Council's Health and Safety policies for using mobile phones.

5.1.3 Users must not use a Council-supplied device for anything that is illegal, for making offensive or threatening calls or whilst driving. All mobile devices should be set up with a Personal Identification Code by the user, to prevent unauthorised use. For instructions on how to do this consult the manual or Admin. Support Team.

5.1.4 The Admin Co-ordinator receives quarterly invoices for each user for all line rental and usage charges. At the same time, each individual user will have a Personal Mobile Phone Statement sent out, usually to their Line Manager, or departmental admin. / clerical contact.

5.1.5 Employees should refer to the Council's Mobile Phone Policy if they require further information.

5.2 Lost or stolen mobile devices

5.2.1 Employees should report lost or stolen mobile devices to the Admin. Support Team or a member of the Admin. Support Team at Broomhill, if the loss is discovered within normal working hours.

5.2.2 If the loss of a device occurs outwith normal working hours, Employees should notify the Vodafone Customer Services 24 hour Help Desk, on 0870 071 1102. Vodafone will immediately bar the phone, and employees must then notify the Admin Co-ordinator or the Admin. Support Team at Broomhill as soon as possible within normal working hours, so that a replacement can be provided.

5.3 Personal calls

5.3.1 Personal calls can be differentiated from business calls by appending an asterisk '*' onto the end of the dialled number. Calls with an appended asterisk will appear on the bill with an asterisk at the end of the number, and so can be more easily identified for recharging purposes. Personal contact numbers can also be stored in the phone or SIM memory with an asterisk at the end.

5.3.2 It is the responsibility of employees and Elected Members to check their statements carefully for personal calls, which should then be refunded to the relevant department.

5.4 Personal text messages

5.4.1 Staff should identify personal text messages on their telephone bills in order that the costs can be paid to the Council.

5.5 Misuse

5.5.1 Employees must not send or receive text messages for downloading, or otherwise accessing ring tones, games, commercial competitions etc. Many of these services operate on an ongoing subscription basis and charge anything up to £5 per item.

5.5.2 There is an automatic bar on all Council mobile devices preventing the dialling of international and premium rate numbers. 'Roaming' to other mobile phone providers networks, for example whilst overseas is also automatically barred.

5.5.3 Employees who are aware of being able to access 'barred' numbers should immediately notify the Admin Co-ordinator or a member of the Admin. Support Team at Broomhill, unless they have been authorised to access such numbers.

5.5.4 Employees needing to access any premium rate numbers in relation to their work, they should contact the Admin Co-ordinator or a member of the Admin. Support Team at Broomhill.

5.5.5 If employees need to dial an international number or to 'roam' networks, an email request should be sent to Admin Co-ordinator or a member of the Admin. Support Team at Broomhill detailing the country for which access is required, and for how long the bar is to be lifted.

6 Use of Electronic Mail

6.1 General

6.1.1 Copying an email to internal or external parties, may breach the Data Protection Act if it reveals all recipients' email addresses to each recipient (e.g. in the case of mailing lists). It can also breach duties of confidentiality (e.g. in the case of emails sent to members of a benefit scheme). Accordingly, it may be appropriate to use the 'BCC' (blind carbon copy) field instead of the usual 'To' or 'CC' (carbon copy) fields when addressing an email. If in doubt, employees or Elected Members should seek advice from their line manager or the Data Protection Officer.

6.1.2 Users are recommended to delete unwanted email to conserve system resources. However the email retention policy will archive on a continuous basis all email messages over 90 days old, these messages are then backed-up and are held indefinitely.

6.1.3 All incoming emails are scanned by a third party on behalf of the Council, using virus-checking software. The software will also block, password protected and encrypted documents, unsolicited marketing email (spam) and emails which have potentially inappropriate attachments. If there is a suspected virus in an email which has been sent to the Council, the sender will automatically be notified and a notice will be received that the email is not going to be delivered because it may contain a virus.

6.1.4 Employees and Elected Members must not set mailbox rules to automatically forward email to an external (i.e. non-Council) mailbox. If you have a business need for remote access to email, request this from your Head of Service via an IT11.

6.2 Attachments

6.2.1 Employees and Elected Members should not send overly large file attachments with their email as they slow down the Council's systems for all users. There are restrictions on the size and type of files employees and Elected Members can transmit between 09:00 and 17:00. The policy regarding acceptable file sizes and file types for both outgoing and incoming mail attachments is listed accordingly.

1. Outgoing File Attachment Size Restrictions:
File size restrictions will be subject to review by the Corporate ICT Manager, as such, the most up-to-date limitations will be published on the Hub.

- Attachments up to 2 megabytes will be transmitted at all times without restriction.
- Attachments greater than 2 megabytes will be held for transmission outwith normal working hours.
- Attachments greater than 20 megabytes will only be transmitted by special arrangement. Contact the ICT Service Desk for advice.
- Messages with more than 5 attachments will be held for transmission outwith normal working hours.

2. Incoming File Attachment Size Restrictions:

- Attachments greater than 50 megabytes will be held for distribution outwith normal working hours.

3. Incoming and Outgoing File Attachment Type Restrictions:

- Allowed:
    - Document Files e.g. (.pdf,.doc,.lwp,.txt)

- Not Generally Allowed:
  - Vulnerable file types e.g. (.csv)
  - Images e.g. (.bmp)
  - Movies e.g. (.mov, .mpg, .avi, .asf)
  - Compressed files e.g. (.zip, .bin, .sit, .sea)
  - Executable files e.g. (.exe, .com, .bat)
  - Sound Files e.g. (.mp3, .wav)

Users requiring special arrangements must contact the ICT Service Desk.

6.3 Business use

6.3.1 Email is not a secure means of communication therefore employees and Elected Members should confirm with the members of the public or contractors that the use of email as a means of communication is acceptable.

6.3.2 In light of the security risks inherent in some web-based email accounts, employees and Elected Members should not email business documents to citizens' or contractors' personal web-based accounts without their express permission to do so.

6.3.3 Under no circumstances should employees and Elected Members send information that would be classified under the Council's Information Classification and Protection Policy as 'RESTRICTED' or 'CONFIDENTIAL' to an external or non-GSi email address. (Contact the Information Security Manager for further details.)

6.3.4 Employees and Elected Members needing to work on documents / data outside of their our normal place of work must ensure that they have taken steps to protect information from theft / loss in proportion to the impact that unauthorized disclosure could have on the Council or citizens. Encrypted USB memory sticks, which are available from ICT, must be used if employees or Elected Members need to take sensitive data about staff or members of the public outwith the office. At all times employees and Elected Members must comply with the Home Working and Information Classification and Protection Policies.

6.3.5 If an email message or attachment contains information which is time-critical, employees and Elected Members should bear in mind that email is not an instant form of communication and may take minutes or hours to arrive. If an email is time-critical, employees and Elected Members should consider telephoning to confirm that it has been received and read.

6.4 Personal use

6.4.1 The Council's email facilities are provided for the purposes of the Council's business, however, the Council accepts that employees and Elected Members may occasionally want to use them for their own personal purposes. This is permitted on condition that all the rules set out in this policy are complied with. Employees and Elected Members must be aware that, if they choose to make use of the Council's ICT facilities for personal correspondence, they can have ***no reasonable expectation of privacy*** because the Council may need to monitor communications for the reasons given in item 11.1.

6.4.2 Personal use of email, in common with the use of the Council's other ICT facilities:

- Must take place outwith working hours i.e. before or after work, during lunch or other breaks.
- Must not interfere with the performance of Council duties;
- Must not take priority over work responsibilities;
- Must not cause unwarranted expense or any liability to be incurred by the Council;
- Should not have a negative impact on the Council in any way; and
- Must be lawful and comply with this policy.

6.4.3 Users must not sign up to receive mailings from companies or organisations unrelated to the Council's business.

6.4.4 Users must not make personal purchases and use their Council email address.

6.4.5 Under no circumstances may the Council's facilities be used in connection with the operation or management of any business other than that of the Council.

6.4.6 While emails in Lotus Notes can be deleted from the 'live' system, emails will have been copied (perhaps many times) onto the backup tapes and in that form may be retained.

6.4.7 By making personal use of the Council's facilities for sending and receiving email employees and Elected Members signify their agreement to abide by the conditions imposed for their use, and signify their consent to the Council monitoring their personal email in accordance with item 11 of this policy.

7 Use of Internet and Intranet

7.1.1 The terms and conditions of third-party websites should be complied with.

7.1.2 The Council trusts employees and Elected Members to use the Internet and Intranet sensibly. Employees and Elected Members should be aware that when visiting an Internet site, information identifying a PC as belonging to the Council may be logged and thereby affect the Council's reputation.

7.1.3 The Council recognises the need for individuals to carry out some personal tasks during working hours, e.g. Internet banking or on-line shopping, and this is permitted subject to the same rules as are set out for personal email use in item 6.4 of this policy.

7.1.4 The following types of files should not be downloaded without authorisation from ICT:

- 'Vulnerable' file types e.g. (.csv)
- Movies e.g. (.mov, .mpg, .avi, .asf)
- Compressed files e.g. (.zip, .bin, .sit, .sea)
- Executable files e.g. (.exe, .com, .bat)
- Sound Files e.g. (.mp3, .wav)

7.1.5 Access to certain websites is blocked. If there is a particular business need to access a blocked site, please follow the procedure for accessing blocked sites which can be found on the intranet.

8 System Security

8.1.1 Security of the Council's ICT systems is of paramount importance. The Council owe a duty to members of the public and contractors to ensure the Council process their details confidentially. It is essential that the Council are able to demonstrate the integrity of information and systems as information might need to be relied upon in court. Employees and Elected Members must take responsibility for the security implications of their use of the Council's ICT facilities.

8.1.2 The Council's ICT facilities must not be used in any way which may cause damage, overloading or which may affect its performance or that of the internal or external network.

8.1.3 All material which is RESTRICTED, CONFIDENTIAL or subject to the Data Protection Act must be kept secure - as directed in the Information Classification and Protection Policy. Such types of information must only be

used for the purposes intended and not disclosed it to any unauthorised third party.

8.1.4 System passwords must be kept safe and not disclosed to anyone. Those who have a legitimate reason to access other users' inboxes must be given permission under the Access to Mailboxes Procedure.

8.1.5 Any Elected Member or employee who receives a call from a member of ICT staff asking for a password, should verify their name on the intranet directory and call them back. Details can also be confirmed with ICT Service Desk.

8.1.6 If a password has to be given to ICT staff, ensure that the password is changed once the ICT employees no longer need it. Contact ICT Service Desk if guidance is needed on how to do this.

8.1.7 Documents should be marked and treated in accordance with the Council's Protective Marking Scheme which is set out in the Information Classification and Protection Policy.

8.1.8 Elected Members and employees must ensure that material from outside the Council which is loaded onto corporate PCs via a disk or CD Rom is from a secure and safe source. If there are any doubts about such material ICT Service Desk should be contacted for assistance. No software should be loaded on to a corporate PC unless it has been authorised by ICT Services.

8.1.9 Programs, applications or software must not be downloaded or installed - regardless of their source - without authorisation from ICT Services. This includes programs, toolbars, instant messaging software, screensavers, photos, video clips and music files. ICT Service Desk are able to offer advice if required.

8.1.10 No device or equipment should be attached to the Council's systems without the prior approval of ICT Services. This includes, cameras, USB flash drives, MP3 players (or similar devices), PDAs or telephones. It also includes use of the USB port, infra-red or any other port.

8.1.11 The Council monitors all emails passing through its system for viruses. However, caution should be exercised when opening emails from unknown external sources or when, for any reason, an email appears suspicious. ICT Service Desk should be informed immediately if a suspicious communication or suspected virus is received.

9 Working Remotely

9.1.1 This chapter and the procedures it sets out, apply to employees and Elected Members use of the Council's ICT facilities, to the use of the Council's laptops, and also to the use of personal computer equipment or third party computer equipment where work is being undertaken away from Council premises. The Council's Home Working Policy contains more details on how to work at home safely and securely.

9.1.2 When working remotely employees and Elected Members must:

- Position themselves so that work cannot be overlooked by another person;
- Switch off laptop computers when not in use or ensure that a password protected screensaver is in place.
- Take reasonable precautions to safeguard the security of the Council's laptop computers or any computer equipment which is used to undertake the Council's business;
- Keep passwords secret;
- Inform ICT Service Desk as soon as possible if a Council laptop / mobile device in their possession or any computer equipment on which Council's work has been undertaken has been lost or stolen;
- Ensure that any work which is done remotely is saved on the Council's system or is transferred to a Council system as soon as reasonably practicable and deleted on any personal device; and
- Password-protect access to any PDAs or similar hand-held devices containing any personal data of which the Council is a data controller or any information relating the Council's business.

9.1.3 An awareness of what information is stored on mobile devices or mobile storage should be maintained so that in the event of a theft or loss, the impact of any compromise of council data can be estimated.

10 Private Blogs and Websites

10.1.1 This part of the policy and procedures in it apply to personal blogs, websites, virtual reality games such as Second Life and all other personal web content (e.g. personal podcasts) even if created, updated, modified or contributed to outside of working hours or when using personal or third-party ICT systems.

10.1.2 Employees and Elected Members may wish to contribute to online forums, blogs and message boards, 'podcast', 'webcast' or similar. For the avoidance of doubt such activities are expressly prohibited during work time or using Council ICT facilities - except where such activities are in pursuance of duties to the Council.

10.1.3 Employees and Elected Members must ensure that any content posted to the Internet, be it written, vocal or visual, which identifies them as a member of the Council and/or discusses their work or anything related to the Council or its business, contractors, members of the public or colleagues, must be appropriate, consistent with their contract of employment and with the Council's policies and procedures.

10.1.4 Employees who already have or contribute to a personal blog or website which indicates in any way that they work for the Council should report this to their line manager.

10.1.5 Employees who intend to create or contribute to a personal blog or website that identifies them as a Council worker should report this to their line manager.

10.1.6 If a blog posting expressing any idea or opinion clearly identifies that an employee works for the Council then a disclaimer should be added such as "these are my own personal views and not those of the Council".

10.1.7 The following matters will be treated as gross misconduct (this list is not exhaustive):

- *Revealing confidential information about the Council*.

This might include revealing information relating to the Council's contractors, business plans, policies, employee, financial information or internal discussions. Managers should be contacted in the first instance to advise on what might be confidential; and

- *Using a personal blog or any website to harass, criticise or embarrass the Council, its clients or employees.*

The reputation of the Council and the privacy and feelings of others should be respected at all times.

10.1.8 Complaints about colleagues or workplace matters should be dealt with by raising a grievance using the Council's Grievance Procedure or by following the Council's 'Whistle-Blowing' policy. Both documents can be found on the Intranet. Employees may also wish to consult their Trade Union;

10.1.9 The Council provides a 'Whistle-Blowing' hotline 0845 0454512, which can be used to raise issues of concern.

10.1.10 Employees or Elected Members who have concerns that something on their blog or website could give rise to a conflict of interest, and in particular raise concerns over issues of impartiality or confidentiality, should discuss this with their line manager.

10.1.11 Employees must talk to their line manager and the Council's Public Affairs Team if the media or press make contact about information on their blog or website relating to the Council.

10.1.12 Personal blogs or websites which do not identify the blogger as a member of the Council and do not mention the Council and are purely concerned with personal matters will normally fall outside the scope of this policy.

11 Monitoring of Communications by the Council

11.1 General Principles

11.1.1 The Council will, so far as possible and appropriate, respect the privacy of employees and Elected Members and their autonomy while working.

11.1.2 The Council may monitor i.e. keep records of email sender, receiver, subject line; attachments to email, telephone numbers called and the duration of calls; domain names of websites visited, the duration of visits, files downloaded from the Internet. The Council may also intercept i.e. record and listen to calls, scan or read emails.

11.1.3 The Council does not routinely intercept telephone calls or routinely *manually* intercept emails. However, emails are automatically scanned for inappropriate content and they will then be subject to manual review.

11.1.4 The Council may carry out the monitoring and interception of business communications for reasons which include:

- Providing evidence of business transactions;
- Ensuring that the Council's business procedures, policies and contracts with are adhered to;
- Complying with any legal obligations;
- Monitoring standards of service, performance, and for training;
- Preventing or detecting unauthorised use of the Council's communications systems or criminal activities; and
- Maintaining the effective operation of the Council's communication systems.

11.1.5 ICT employees who operate and support electronic communications facilities need, from time to time, to monitor transmissions or observe transactional information to ensure proper functioning of Council facilities and services. On these and other occasions, such personnel might inadvertently become aware of the contents of electronic communications. Except as provided for under the terms of this policy and the Lawful Business Practice Regulations, employees are not permitted to intentionally examine the contents of communication or disclose or otherwise use what they have seen, heard or read. However, if violations of Council policies or law are discovered, employees should report these to their line manager.

11.1.6 It is not possible for the Council to distinguish between personal and business communications so staff must be aware that monitoring and any interception may cover both personal and business communications for the purposes specified at item 11.1.1

11.1.7 Employees and Elected Members need to be aware that such monitoring might reveal sensitive personal data about them. For example, if they regularly visited websites which contained information about health or sexuality, or which detailed the activities of a particular political party or religious group, then those visits might indicate their health, sexual orientation, political opinions or religious beliefs. By carrying out such activities using the Council's ICT facilities employees consent to the Council's holding and processing of any sensitive personal data about them which may be revealed by monitoring. Data on sites visited is kept for up to 3 years and is collected for the purposes of ensuring that the Council's policies are complied with.

11.1.8 Sometimes it is necessary for the Council to access employees' business communications during their absence, such as when they are unexpectedly taken ill, or while they are on holiday. Unless mailbox settings are such that the individuals who need to access mail can

already do this, access will be granted only with the permission of a Head of Service.

11.2 Personal Communications

11.2.1 Employees must abide by the terms of use set out in Chapter 6 of this policy.

11.2.2 Only web-based email services with appropriate security measures are permitted all others are strictly forbidden. The list of permitted providers is published on the Hub.

11.2.3 Employees and Elected Members are responsible to any third-party who sends them, or receives from them, a personal email, for the consequences of any breach of that third-parties' privacy which may be caused by that employee's or Elected Member's failure to follow this policy.

12 Data Protection

12.1.1 Employees and Elected Members will inevitably be involved in processing personal data for the Council. The Data Protection Act 1998 sets out the rules governing the privacy of individuals' data. The following terms defined by the Act:

- "Data" refers to information which is computerised or in hard copy form;
- "Personal data" is data which can identify a living individual, such as a name, a job title, a photograph;
- "Processing" is anything done with data – just having data amounts to processing; and
- "Data controller" is the person who controls the purposes and manner of processing of personal data – this will be the Council, in the case of personal data processed for business purposes.

12.1.2 Personal data processed by the Council must be kept confidential and secure, and must take particular care not be disclosed to any other person (whether inside or outside the Council) without authorisation. Personal data must only be used by the Council for the purposes for which it was collected. The Council's FoISA and Data Protection Officer or line managers can be contacted for advice.

12.1.3 Emails or documents relating to Council business, containing personal information covered by the Data Protection Act, should not be sent outside of the European Economic Area without first consulting the

FoISA and Data Protection Officer.

12.1.4 The 1998 Act gives every individual the right to see all the information which any data controller holds about them, subject to certain exemptions. Employees and Elected Members should bear this in mind when recording personal opinions about someone. Personal remarks and opinions must be made or given responsibly, and must be relevant, appropriate as well as accurate and justifiable.

12.1.5 Section 55 of the 1998 Data Protection Act states that it is a criminal offence knowingly or recklessly to obtain or disclose personal data without the consent of the data controller, unless this is necessary to detect or prevent crime, or is authorised by another statute or rule of law. "Obtaining" would include the gathering of personal data by employees at work without the authorisation of the Council. This offence may be committed, if without the appropriate authority, employees and Elected Members:

- exceed their authority in collecting personal data;
- access personal data held by the Council; or
- pass data on to someone else (whether inside or outside the Council).

12.1.6 While the Council is data controller of all personal data processed for the purposes of the Council's business, employees and Elected Members will be data controller of all personal data processed in any personal email which they send or receive. Use for social, recreational or domestic purposes attracts a wide exemption under the 1998 Act, but if, in breach of this policy, the Council's communications facilities are being used for the purpose of a business which is not the Council's business, then extensive personal liability under the 1998 Act will be taken on by an employee or Elected Member.

12.1.7 To help you understand and comply with the Council's obligations as data controller under the 1998 Act employees and Elected Members may be offered, or may request, training. In the event of any uncertainty over the requirements of the Data Protection Act, the Council's Data Protection Officer should be contacted. The Council's privacy statements and information about the Council's data protection policies can also be found on the Hub.

13 Inappropriate Use of ICT Facilities

13.1 General

13.1.1 Misuse or abuse of the Council's ICT facilities in breach of this policy will be dealt with in accordance with the Council's disciplinary

procedure.

13.1.2 The receipt of inappropriate material or instances of misuse of Council ICT facilities should be reported to ICT Service Desk or the relevant line manager.

13.1.3 Access to ICT facilities may be suspended without warning pending investigations of suspected misuse and may be removed altogether if a breach of the ICT policy is found. Where potentially illegal material is found to be viewed or stored on any Council ICT facility, the Police should be informed immediately in coordination with the Information Security Manager.

13.1.4 Employees and Elected Members must not forward on material which they feel is inappropriate or seek to investigate suspected misuse themselves. Such matters should be referred to the Information Security Manager or Human Resources via their line manager.

13.1.5 The following would be considered 'misuse' that could result in disciplinary action. This list is indicative, not exhaustive:

- Breaching the Council's security policies;
- Accessing, downloading, installing or distributing offensive, obscene or indecent material e.g.: pornography, racist or sexist material and violent images;
- Accessing, downloading, installing or distributing material likely to be of use in the commission of a crime;
- Using images, text or material which are copyright-protected, other than in accordance with the terms of their license;
- Using Council ICT facilities to convey messages which contain expletives, threats or defamatory or discriminatory statements;
- Excessive private use of email, Internet, telephones, faxes or any other Council ICT facility;
- Entering into contracts, in breach of the Council's standing orders, without authority by using the Council's name in emails or on the Internet;
- Accessing or using unauthorised personal web based email accounts
- Accessing or using instant messaging software or other similar services;
- Accessing or using Internet chat rooms;
- Downloading or forwarding software, games or programs without the authorisation of ICT Services;
- Installing or storing any executable files (e.g. .exe, .scr or.com) without proper authorisation

- Changing the configuration or set up of Council ICT facilities in such a way as to impair their operation, without proper authorisation from ICT Services;
- Removing or interfering with the cabling or power supply of any ICT facilities so as to impair its operation, without proper authorisation;
- Attaching any device e.g.: USB memory sticks, PDA's, Blackberries etc. to an EDC ICT facility which has not been specifically approved by ICT Services;
- Breaching or attempting to breach the security of any ICT facility;
- Sharing passwords or permitting others to access an ICT facility that has been assigned to their use, without proper authorisation;
- Removing ICT equipment or software from Council premises without proper authorisation;
- Accessing another user's email or personal files without the knowledge of the user or outwith the terms of the Access to Mailboxes Procedure;
- Accessing or trying to access data which is known to be, or could be reasonably expected, to have been known to be confidential;
- Disclosing or trying to access data which is known to be, or could be reasonably expected, to have been known to be confidential;
- Introducing deliberately any form of viruses or 'malware', i.e. software with malicious intent, into any ICT system
- Introducing packet-sniffing, keystroke logging or password-detecting software;
- Seeking to gain access to restricted areas of the Council's network; and
- Encrypting or password protecting important data or files to which other require access.

13.2 Computer Misuse Act 1990

13.2.1 Hacking, i.e. attempting to gain unauthorised access into Council ICT facilities is a crime and could lead to your prosecution under the Computer Misuse Act 1990, which creates the following offences:

- Unauthorised access to computer material
- Unauthorised modification of computer material; and
- Unauthorised access with intent to commit or facilitate the commission of further offences.

13.2.2 ICT staff must not attempt to recreate or emulate a security incident without authorisation as this can also constitute a breach of this policy or an offence.

East Dunbartonshire Council

14 SECTION 2: Acceptable Use Guidelines for Members of the Public Using Council Information and Communication Technology (ICT) and Internet Facilities

14.1 ICT and Internet Use: Libraries and Community Centres

In order to meet the information, educational, recreational and cultural needs of its residents, students, visitors and people who work in East Dunbartonshire, the Council provides free access to a wide range of resources in designated public buildings.

To ensure the benefits of the information age are open to all, free access to Information and Communications Technology (ICT) and the Internet is provided by the Council within Libraries and Community Centres. Facilities include a range of computer services, for instance word processing, spreadsheets, CD-Rom databases etc.

Sessions can be booked in multiples of an hour. Sessions cannot exceed one hour if another user wishes to book a session. A booking will be held for ten minutes from the start time and if not claimed may be booked by another user.

Staff may be available to provide assistance. In Libraries, staff can help with the booking of sessions for advanced training and assistance.

Current charges for printouts etc are displayed in Libraries.

14.2 General

The Internet is a portal to online resources from all over the world. The resources available are changing the way individuals access information and communicate with each other.

In addition to providing access to the World Wide Web, the Council provides access to other Internet services such as email and newsgroups.

The Internet is a global electronic network and East Dunbartonshire Council does not have any control over the information available and is not responsible for the accuracy, validity, legality or usefulness of the information available. The Council accepts no responsibility for the quality or reliability of the telecommunications links upon which the service depends, and which are outside its control. The Council has installed filtering software to try and prevent access to illegal sites, but you should realise filtering only gives limited protection.

Parents, guardians and carers should be especially vigilant to work with children, young people and supported individuals and groups to ensure responsible use. Further information on the Internet is available in “A Parent’s and Carer’s Guide to the Internet” and “A Guide to the Internet for Supported Individuals and Groups”.

Email facilities can be accessed via free web-based mail services such as www.hotmail.com and www.yahoo.co.uk. No personal email will be stored on the hard disk of the Council PCs and no personal address books will be stored.

Any financial transactions, including costs incurred, are the responsibility of the users and are carried out at the users' own risk.

All floppy disks, or other authorised removable media, must be virus checked before use.

Individuals a re responsible for their use of ICT and the Internet, and must respect the privacy of others. Breaching this policy may result in access to ICT facilities and the Internet being withdrawn, and may result in prosecution.

Monitoring of computer systems and networks is necessary to maintain optimum performance of the service. The Council monitors and logs all aspects of its computer systems and networks, including Internet sites and newsgroups visited by users, and the downloading of files of all types. Also, the Council reserves the right to restrict the types of files you can download.

Health and safety advice on computers is available on request.

14.3 Prohibited Behaviour

You must not, or as a responsible adult you must not, allow those under your care to:-

- Access the ICT or Internet facilities except as authorised under this policy.
- Access ICT for any illegal activities including the creation and distribution of illegal materials including obscene, offensive, indecent or menacing material.
- Access the Internet for any illegal activities, or for viewing or distributing illegal materials including obscene, offensive, indecent or menacing material.
- Violate copyright laws by unauthorised reproduction or distribution of copyright or licensed material. If in doubt, check with the copyright holder or the owner of the material.
- Engage in any activity which is offensive or which invades another person's privacy.
- Restrict or inhibit other users from using the system or impair the efficiency of the computer, its security measures or its operating system.
- Save documents and / or software on the hard drive.
- Damage, delete, impair or otherwise harm the ICT hardware or software.

If you access an Internet site whose contents alarm you, or you see another user doing so, please inform a member of the staff immediately.

14.4 Procedures for use in Libraries

You do not need to be a member of the library to use ICT and Internet facilities.

If you are already a member of the library service you should register to use ICT / Internet services. If you choose not to join the library, you will be required to sign a copy of these Acceptable Use Guidelines every time you wish to use one of the library's computers.

Signing the consent form to book a PC automatically enables use of the Internet. If you are under 16, we require a signed consent form from your parent or guardian.

Library staff are willing to assist you in using a PC. Library staff, however, are not trained to provide tuition. If you require teaching support, library staff will be happy to pass your details to staff responsible for running tutorials in computing skills. Forms are available in each library for this purpose.

14.5 Procedures for accessing ICT and Internet facilities in Community Centres and other LearningCentres

ICT and internet facilities in community centres may be accessed by community centre customers. The following procedures shall be managed by the Community Learning and Development Team. The procedure for the use of ICT and Internet facilities depends upon whether or not the use is supervised by an EDC staff member.

General Procedure

The use of ICT and internet facilities in community centres shall only available to community centre customers. Community centre customers are organisations that let out spaces in the community centre. Organisations shall generally mean groups or bodies that are formally constituted. The use of ICT and internet facilities shall only be granted to community centre customers that have first booked the 'computer room' in the community centre; that is the space in the community centre where the ICT and internet facilities are located. Only one community centre customer shall be granted use of the ICT and internet facilities at any one time. Where practical the space in which the ICT and internet facilities are located shall be locked when not in use. Customers seeking to book the computer room should complete a 'school and community centre let application form' and submit it to the Letting Office at: Community Learning and Development, 36 Roman Road, Bearsden, G61 2SQ.

All individuals, forming the membership of the customer organisation, wishing to use the ICT and internet facilities shall be required to read the Acceptable Use Guidelines and sign the appropriate User Agreement Form, undertaking

that the individual has read and shall comply with the Acceptable Use Guidelines. The completion of the User Agreement Form requires proof of address to be shown to a member of the EDC letting team or the centre site coordinator. Should the individual be under 16 or require support in using ICT facilities separate form must to be signed by a parent or guardian.

Unsupervised use

The following procedure applies in circumstances where a customer shall use the ICT and Internet facilities without the supervision of an EDC staff member. All individuals, forming part of the customer organisation, having signed the acceptable use policy, shall be issued with a username and password by the letting team. This username and password shall be for the sole use of the individual and must not be shared with anyone else. As part of the issue of a username and password the individual shall be required to supply answers to some security questions. This information shall be used to reissue a username and password should the individual forget their username or password.

An individual may only use their username and password to log onto a computer at times when their organisation has booked out the 'computer room'. An individual user must note their use of a computer in the log-in sheet provided. As noted above all individuals are required to sign and adhere to the Acceptable Use Guidelines.

Supervised Use

The following procedure applies in circumstances where a customer uses ICT and internet facilities under the supervision of a member of EDC Staff; for example an EDC run youth club or computer course. In such circumstances the EDC staff member shall be given a generic username and password for all individuals participating in the supervised activity to use. As noted above all individuals are required to sign and adhere to the Acceptable Use Guidelines. Users must not share this generic username or password to other members of the public. Users must also not use this generic username and password at times when the use of the ICT and internet facilities is not supervised. In order to reduce the risk of generic usernames and passwords becoming known to non participants, generic usernames and passwords shall be changed periodically. An individual user must note their use of a computer in the log-in sheets provided.

Milngavie Youth Café and other Learning Centres

The Milngavie Youth Café is an EDC supported youth facility with ICT and internet facilities. All activity within the Cafe is supervised by EDC staff members. All individual users shall be required to sign and adhere to the Acceptable Use Guidelines as described above. Thereafter the procedures pertaining to supervised use must be followed

Acceptable Use of ICT and Internet Facilities

Only after compliance with the above procedures may individuals use the ICT and Internet facilities in community centres. A breach of the Acceptable Use Guidelines may result in access to ICT facilities and the Internet being withdrawn and may lead to prosecution.

East Dunbartonshire Council

15 Information and Communication Technology (ICT) and Internet Facilities User Agreement for Children and Young People (under 16)

If you wish your child to be able to use the ICT Services in Libraries / Community Centres, please read A Parent and Carer's Guide to the Internet. You should then complete and sign this form.

- I have read and agree to abide by the policies regarding the use of East Dunbartonshire's ICT provision in public buildings
- I agree to pay for any repair or replacement costs of equipment or software damaged by myself or by anyone for whom I am responsible.
- I understand that the Council is not responsible for any damage or loss of information due to system malfunction, or any other reason.
- I understand that my child's failure to abide by the Acceptable Use Guidelines, may result in loss of access.

Name of child/young person (print):	
Address of child/young person:	
Town:	
Postcode:	
Telephone number:	
Date of birth:	
Signature	Date

As parent/guardian (delete as appropriate) of the individual named above, I give permission for him/her to use the service.

Name of child/young person (print):	
Address of child/young person:	
Town:	
Postcode:	
Telephone number:	
Signature	Date

If your child is not a member of the Library Service you will have to complete this form every time they use the Service in the library. We hope you will decide to join the library.

If you wish further advice on children and young people's use of the Service, please email libraries@eastdunbarton.gov.uk.

Information on this form may be processed by computer under the provisions of the Data Protection Act.

East Dunbartonshire Council

Parent and Carer's Guide to the Internet in Libraries.

East Dunbartonshire Council provides Internet access for children and young people. If you wish your child to make use of the service, you must sign a consent form. To ensure that the experience is as informative and safe as possible, parents/carers are urged to read the following guidance and information.

The Internet
The Internet is an important resource, which enables computers to connect to computers all over the world via a telephone connection. Trained staff will be able to offer advice on how to access this resource, and to recommend websites for children and young people.

The Advantages
It is generally recognised that the best learning is done while having fun and sites on the World Wide Web can offer a fun and interactive learning experience. The World Wide Web makes it possible to do research, tour museums, play interactive games or get help with homework. Children and young people can also acquire important ICT skills.

The Disadvantages
There are no guarantees to the quality of accuracy of material available on the World Wide Web and it is not always the best source of information. While east Dunbartonshire Council uses filtering systems to reduce the risk of coming across material generally considered inappropriate, no system is foolproof.

Personal safety is an important issue, as children and young people may come across sites which make them uncomfortable, or ask them to give personal details.

The Recommendations
While there is a risk in allowing children and young people access to the Internet, it can be greatly minimised by educating them in the principles of Safe Surfing, and by ensuring that parents/carers and council, services work together to apply common sense guidelines. Parents/carers are encouraged to spend online time with their children.

Before children use the library ICT and Internet facilities for the first time, they will be asked to complete a short quiz on how to make the safest use of the Internet.

Ultimately, the Internet use of children and young people is the responsibility of the parent/guardian.

Further Information
If you would like more information, there are a number of other resources available. Some suggestions can be found on the Council website, bookmarked sites on Library PCs, or on a list available from the library. Alternatively you can look at the following sites:

http://www.thinkuknow.co.uk
http://www.nch.org.uk/information/index.php?i=209
http://www.parentscentre.gov.uk/usingcomputersandtheinternet/

If you would like more information please e mail libraries@eastdunbarton.gov.uk
Information on this form may be processed by computer under the provisions of the Data Protection Act.

East Dunbartonshire Council

16 Information and Communication Technology (ICT) and Internet Facilities User Agreement for Adults (16 and over)

- I have read and agree to abide by the policies regarding the use of East Dunbartonshire's ICT provision in public buildings
- I agree to pay for any repair or replacement costs of equipment or software damaged by myself or by anyone for whom I am responsible.
- I understand that the Council is not responsible for any damage or loss of information due to system malfunction, or any other reason.
- I understand that if I fail to abide by the Acceptable Use Guidelines, I may lose the right of access.

Name of child/young person (print):	
Address of child/young person:	
Town:	
Postcode:	
Telephone number:	
Date of birth:	
Signature	Date

If you are not a library member, you will have to fill this form in every time you wish to use the service in the library. We hope you will decide to join the library.

Information on this form may be processed by computer under the provisions of the Data Protection Act.

East Dunbartonshire Council

Information and Communication Technology (ICT) and Internet Facilities User Agreement for Someone Acting on Behalf of Supported Individuals or Groups

If you wish a supported individual or group for whom you are responsible to be able to use the ICT and Internet facilities, please ensure that you have read and understood both this document and the "Guide to the Internet for Supported Individuals and Groups". You should then complete and sign this form.

- I have read and agree to abide by the policies regarding the use of East Dunbartonshire's ICT provision in public buildings
- I agree to pay for any repair or replacement costs of equipment or software damaged by myself or by anyone for whom I am responsible.
- I understand that the Council is not responsible for any damage or loss of information due to system malfunction, or any other reason.
- I understand that failure by the supported individual or a member of the group for which I am responsible to abide by the Acceptable Use Guidelines may result in the loss of access.

As the person responsible for the supported individual or group named below, I give permission for him/her to use the Service.

Name of supported individual or group:	
Your name (print):	
Your address:	
Town:	
Postcode:	
Signature	Date

If the person for whom you are responsible is not a member of the Library Service, you will have to complete this form every time you use the ICT and Internet Service in the library. We hope that you will persuade the person concerned to join.

Information on this form may be processed by computer under the provisions of the Data Protection Act.

East Dunbartonshire Council

A Guide to the Internet and Supported Individuals: Carer's Guide to the Internet.

East Dunbartonshire Council provides Computing and Internet access for everyone. If you wish someone in your care to make use of the service, you must sign a consent form. To ensure that the experience is as informative and as safe as possible, carers are urged to read the following guidance and information.

The Internet
This is an important resource, which enables computers to connect to computers all over the world via a telephone connection. Library staff will be able to offer advice on how to access this resource, and to recommend websites.

The Advantages
The World Wide Web makes it possible to do research, tour museums, play interactive games or get help with homework. Anyone can acquire increasingly important ICT skills. It is generally recognised that the best learning is done while having fun.

The Disadvantages
There is no editing of material available on the World Wide Web. It may be inaccurate or inappropriate. Web browsing is not always the best way to find out something. While East Dunbartonshire Council will use filtering systems to block access to material generally considered offensive, no system is foolproof. Personal safety is another issue, as people may come across sites which make them feel uncomfortable, or be asked to give personal details.

The Recommendations
While there is a risk in allowing access to the Internet, it can be greatly minimised by educating them in the principles of Safe Surfing, and by ensuring that carers and council services work together to apply commonsense guidelines.

Carers are encouraged to spend time on-line with the person or people in their care. This is because using a PC in an East Dunbartonshire Library automatically provides access to the Internet. Carers and guardians should consider these points carefully before signing the consent form, as this give access to the Internet.

Ultimately, Internet use by a person in your care is the responsibility of the carer.

If you wish further advice please e mail libraies@eastdunbarton.gov.uk

East Dunbartonshire Council

17 SECTION 3: Acceptable Use Guidelines for Young People in Schools a Guide for Pupils and Parents

The computer systems in the schools are owned by East Dunbartonshire Council and are made available to young people to further their education. Attached is a copy of the school rules that will be displayed at appropriate places in the school. These rules will be explained to all young people by staff in school.

The school and local authority may exercise its right by electronic means to monitor use of the school's computer systems, including monitoring websites, interception of electronic mail and deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or maybe taking place or, where there is concern that the system may be being used for criminal purpose or for storing text or imagery which is unauthorised or unlawful.

- ☒ Access to the network must be made via the user's authorised account and password, which must not be given to any other user
- ☒ School computer and internet use must be appropriate to learning
- ☒ Young people should report any information or messages that they receive which they are concerned about to a member of staff.
- ☒ Copyright of materials must be respected
- ☒ Users are responsible for electronic messages that they send and for contacts made
- ☒ Electronic mail should be written carefully and politely. As messages may be forwarded, electronic mail is best regarded as public property.
- ☒ Anonymous messages and chain letters must not be sent
- ☒ The use of public chatrooms is not allowed. Restricted use of authorised chatrooms is allowed with the permission and monitoring of a member of staff.
- ☒ Electronic mail or websites must not be used as a means of bullying people
- ☒ The school network may not be used for private purposes, unless permission has been given by the Head Teacher
- ☒ Use for personal financial gain, gambling, political purpose or advertising is forbidden
- ☒ Only information relevant to the curriculum may be downloaded from the network
- ☒ The school and the local authority reserve the right to check computer files and monitor Internet sites that are visited
- ☒ Users must not try to breach the security measures that are in place on the Council's systems
- ☒ Irresponsible use may result in the loss of computer, Internet and email access

East Dunbartonshire Council

18 Rules for Safe Use of Computers in Primary Schools

- ☒ On a network, I will use only my own login and password, which I will keep a secret
- ☒ I will not look at or delete other people's files
- ☒ I will only use computers for school work and homework
- ☒ I will not put anything in the computer unless I have been given permission
- ☒ I will ask permission from a member of staff before using the Internet
- ☒ I will only email and send messages to people I know, or my teacher has approved
- ☒ The messages I send will be polite and responsible
- ☒ I will not use chatrooms or Internet chat unless given permission by a teacher.
- ☒ When sending email, I will not give my home address or telephone number, or arrange to meet someone
- ☒ I will ask permission before opening an email or an email attachment sent by someone I do not know
- ☒ I will remember that some material on the Internet is copyright protected
- ☒ I will only download files that I need for school work
- ☒ If I see anything I am unhappy with or I receive messages I do not like, I will tell a teacher
- ☒ I know that the school may check my computer files and the Internet sites that I have visited
- ☒ I understand that if I deliberately break these rules, I could be stopped from using the computer, Internet and email

East Dunbartonshire Council

19 Rules for Safe Use of Computers in Secondary Schools

- ☒ At all times access the computer network with your own log-in and password and do not tell anyone what this is
- ☒ Do not attempt to access other people's files
- ☒ Use computers for school work and homework only
- ☒ Do not plug devices in to school computers unless you have permission from a teacher
- ☒ Do not use material which is copyright protected
- ☒ Download only from sites relevant to school work
- ☒ Ensure that you have permission to access the Internet
- ☒ Remember that you are responsible for email you send and for contacts made Email only people that you know or contacts that the teacher has approved
- ☒ Email should be written carefully and politely
- ☒ Do not send anonymous messages or chain letters
- ☒ Use of public chat rooms is not allowed
- ☒ Do not give out any personal details including home address, telephone number, or arrange to meet someone
- ☒ Report any unpleasant or offensive material or messages to a member of staff. This report will be confidential and will help to protect all system users
- ☒ Use for personal financial gain, gambling, political purposes or advertising is forbidden
- ☒ Remember that the school may check your computer files and may check the Internet sites that you have visited
- ☒ Irresponsible use may result in loss of computer, Internet and email access

East Dunbartonshire Council

20 School Internet and Email Permission Form

Dear Parent/Guardian,

Access to the Internet and email is now a recognised and valued educational tool which all schools in East Dunbartonshire Council have access to. Before being allowed to use the Internet, pupils must obtain parental consent and I would ask you and your son/daughter to sign and return the enclosed form as evidence of your approval and their acceptance of the schools rules on this matter.

Access to the Internet will allow your child to explore thousands of libraries, data bases and bulletin boards while being able to exchange email messages with other Internet users throughout the world. Our aim in using the Internet is in pursuit of educational goals but some pupils may try to find information that is not consistent with our aim. A filtering system has been put in place which has been designed for safe usage in education. During school hours teachers will guide pupils in their use of the Internet and all pupils engaged on using the Internet will be supervised.

It is considered that the educational benefits of Internet and email access far exceed the disadvantages. While some material on the Internet contains items which are illegal, offensive, inaccurate or morally unacceptable to some people, East Dunbartonshire Council has taken all practical steps to ensure safe use that the risks of your child being exposed to such material are minimised. Ultimately parents and guardians are responsible for setting the standards that their children should follow when using media and information sources. The school supports and respects each family's right to decide whether to apply for access or not.

Please read the enclosed guidance documents and then complete the permission form which follows. This should be returned to the school before the _____. If forms are not returned by the due date we will assume that access is not being applied for and therefore will not be granted.

East Dunbartonshire Council

Parental/Guardian Agreement

☒ As the parent or legal guardian of the pupil signing below, I grant permission for my son or daughter to use electronic mail and the Internet

☒ I understand that pupils will be held accountable for their own actions

☒ I am aware that East Dunbartonshire Council will take all possible precautions to eliminate unsuitable materials but accept that it is impossible for the school to guarantee elimination of all sources of controversial material

☒ I accept responsibility for setting standards and explaining the enclosed set of rules for my child to follow when selecting, sharing and exploring information and media and I understand that any misuse of the system will result in my child being barred from the electronic mail and the Internet.

☒ I understand that this policy is also applicable when my child is using any computer outwith an East Dunbartonshire Council school to access the National Educational Portal (GLOW).

I hereby give you permission to issue electronic mail and Internet access to my child.

Parent/Guardian Name
(please print) _____

Pupil Name and Class _____

Signature _____ Date_____

Pupil Agreement (Pupils 16 and over only)

As a school user of electronic mail and the Internet, I agree to comply with the school rules on their use. I will use the network in a responsible way and observe all the restrictions explained to me by my parent/guardian and the school. I understand that should I breach the rules then my access will be removed and disciplinary action may result.

Pupil Name
(please print) _____ Class_____

Pupil Signature _____ Date_____

East Dunbartonshire Council

21 SECTION 4: Use of the Internet by Young Children in Early Years Settings

RATIONALE:

The internet plays an increasingly important part in our society today. Young children may have experience of watching their parents ordering goods or services from the internet, banking online or sending email. They may have seen older siblings use the internet for entertainment, such as playing games or downloading music.

There are many benefits for young children learning via the internet. It can be a useful source of information, helping staff to research a topic in response to children's interests. It offers access to a vast range of resources, many of which can be downloaded free of charge. For example, staff can download samples of music from other cultures, pictures of castles or short videos of minibeasts to support and enhance children's learning. The internet offers a wide variety of games at various levels, to allow for differentiation. These can offer new ways to stimulate children's interest and to motivate them towards learning.

However, there are also some potential problems, including unsuitable sites, aggressive advertising, pop up windows showing adult content and links to other sites.
The internet contains vast amounts of information on virtually every subject imaginable. Just as a library has sections which appeal to different readers, not all the information on the internet may be suitable for young learners. Some of the content may be unreliable or misleading.

The policy guidelines which follow are designed to promote safe use of the internet by young children in early years settings within East Dunbartonshire.

RESOURCES

Early Learning, Forward Thinking: The ICT Strategy for Early Years, Learning and Teaching Scotland, 2004 *Double Click Thinking,* Scottish Executive http://www.ltscotland.org.uk/doubleclickthinking/ *The Internet and Young Children,* National Association for the Education of Young Children, 1998 http://www.naeyc.org/ece/1998/18.asp

CROSS REFERENCES

The Child at the Centre	6.2
National Care Standards	2.4

East Dunbartonshire Council

Policy Guidelines for the Use of the Internet by Children in Pre-School Settings within East Dunbartonshire.

- **Permission should be obtained from parents before using the internet with their child**.

- **Staff should supervise young children's use of the internet.** Within East Dunbartonshire Council, access to the internet will not be provided in accounts set up for pre-school children's use of the computers. Staff should log in on their own accounts to access the network, and then log out after using the internet with the children.

- **Staff should check the content of websites before using them with young children.**
  Once a suitable site has been identified, this should be added to the Favourites list, to give quick direct access.

- **Staff should check the source of the information.** Even if it appears to come from a reputable source, for example a university, it is worth looking for the tilde sign **~** in the URL (shown in the address box) as this usually indicates areas of a website relating to an individual, whose views might be totally different from those held by the university.

- **Filtering software should be installed to block unsuitable content**. Staff should be aware that despite the best endeavours to ensure security, it may still be possible that some unsuitable content could be accessed. Any breaches of the security should be reported immediately by logging on the Help Desk, so that this can be investigated and the problem rectified.

- **Pre-school children will not have direct access to email within early years settings in East Dunbartonshire Council.**
  On occasion, it may be desirable to communicate by email, for example to share news with children in another early years setting. This may be carried out as a joint learning experience involving children and a member of staff, via the staff member's email account.

  By taking responsibility for children's computer use, families and early childhood professionals can greatly reduce the potential associated risks, while at the same time allow children access to a multitude of positive learning experiences.
  National Association for the Education of Young Children (1998)

East Dunbartonshire Council

Dear Parent /Guardian

INTERNET PERMISSION FORM

Access to the internet is now a recognised and valued educational tool which all schools and local authority early years settings in East Dunbartonshire Council have access to. Before your child can access the internet under the supervision of a staff member, your consent is required. Please sign and return the enclosed form as evidence of your approval and acceptance of the policy guidelines on this matter.

Access to the internet will allow your child a much wider range of pre-selected resources and activities which can support and enhance their learning. This could include games, photographs, short video clips, music and other sound files. Staff may use the internet to find information in order to respond to a child's question or to help develop one of the children's interests. A filtering system has been put in place, with the best endeavour to block unsuitable content. Your child will always be supervised by a staff member who has checked the site before visiting it with your child.

It is considered that the educational benefits of internet access far exceed the disadvantages. While some material on the internet contains items which are illegal, offensive, inaccurate or morally unacceptable to some people, East Dunbartonshire Council has taken all practical steps to ensure safe use. The centre supports and respects each family's right to decide whether to apply for access or not.

Please complete the permission form which follows. If forms are not returned by the due date, we will assume that access is not being applied for and therefore will not be granted.

Further information is available from the Scottish Executive's Double Click Thinking website at
http://www.ltscotland.org.uk/doubleclickthinking/

East Dunbartonshire Council

PARENTAL CONSENT FORM FOR PRE-SCHOOL CHILDREN'S ACCESS TO THE INTERNET

I give/do not give* my consent for my son/daughter*

_____ (insert child's full name) to use the internet within the early years centre, accompanied by a member of staff.

Name_____
(Please print)

Signed_____

Date_____

Relationship to Child_____

Please return this form to the early years centre by

_____

- delete as appropriate

East Dunbartonshire Council

22 SECTION 5: A Parent and Carer's Guide to the Internet

East Dunbartonshire Council provides Internet access for children and young people. If you wish your child to make use of the service, you must sign a consent form. To ensure that the experience is as informative and as safe as possible, parents/carers are urged to read the following guidance and information.

The Internet
The Internet is an important resource, which enables computers to connect to computers all over the world via a telephone connection. Trained staff will be able to offer advice on how to access this resource, and to recommend websites for children and young people.

The Advantages
It is generally recognised that the best learning is done while having fun and sites on the World Wide Web can offer a fun and interactive learning experience. The World Wide Web makes it possible to do research, tour museums, play interactive games or get help with homework. Children and young people can also acquire important IT skills.

The Disadvantages
There are no guarantees to the quality or accuracy of material available on the World Wide Web and it is not always the best source of information. While East Dunbartonshire Council uses filtering systems to reduce the risk of coming across material generally considered inappropriate, no system is foolproof.

Personal safety is an important issue, as children and young people may come across sites which make them feel uncomfortable, or ask them to give personal details.

The Recommendations
While there is a risk in allowing children and young people access to the Internet, it can be greatly minimised by educating them in the principles of Safe Surfing, and by ensuring that parents and council services work together to apply common sense guidelines. Parents/carers are encouraged to spend time on-line with their children.

Before children use the library Internet facilities for the first time, they will be asked to complete a short quiz on how to make the safest use of the Internet. Young people in youth facilities will participate in group activity sessions to discuss the principles of safe surfing.

Ultimately the Internet use of children and young people is the responsibility of their parent/guardian.

Further Information
If you would like more information, there are a number of other resources available. Some suggestions can be found on the Council Website, bookmarked sites on Library PCs, or on a list available from the library. Alternatively, you can look at the following sites:

- http://www.thinkuknow.co.uk
- http://www.nch.org.uk/information/index.php?i=209
- http://www.parentscentre.gov.uk/usingcomputersandtheinternet/