



Ysgol Gynradd Brynhyfryd Primary School

"Breuddwydio, credu, llwyddo gyda'n gilydd!"

"Dream, believe, achieve together!"

Brynhyfryd Primary School is a Rights Respecting School

SCHOOL POLICY DOCUMENT

ICT ACCEPTABLE USE POLICY

Reviewed:

Approved by Governors:

Next Review:

ICT Acceptable Use Policy

Contents

1. Policy statement
2. Scope and general use
3. Security information
4. Using the internet, email, instant messaging, video conferencing and Skype for business
5. Social media and networking
6. Telephones and fax machines
7. Mobile phones
8. Reference documentation

1. Policy Statement

1.1 Advances in technology allow City and County of Swansea (CCoS) staff to carry out their work and communicate with colleagues and customers in a variety of ways. It is the responsibility of all staff to know these guidelines and to conduct their activities accordingly.

1.2 The purpose of this policy is to outline the acceptable use of all ICT equipment and facilities within the CCOS. All council staff are required to use the ICT equipment and facilities provided in an appropriate and professional manner.

1.3 Inappropriate use exposes the Council to risks including virus attacks, compromise of network systems and services and, potentially, legal issues. Failure to comply with the policy or abuse of the system may result in facilities being withdrawn and disciplinary action being taken.

1.4 This policy covers the use of all ICT systems including:

- internet, email, instant messaging, video conferencing and skype for business
- Telephones
- Mobile phones, and
- Fax machines

1.5 This policy refers to any type of device staff are using to conduct Council business.

2.0 Scope and general use

2.1 This policy applies to all staff other than those in educational establishments with delegated powers. It also applies to all equipment and systems owned or leased by CCOS. The Council will monitor the application of this policy and has discretion to review it at any time through the appropriate consultation mechanisms. January 2016

2.2 While CCOS wishes to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of CCOS. Because of the need to protect CCOS's network, it may be necessary to scan or monitor information stored on any computer, PDA or networked device belonging to the Council.

2.3 This policy recognises that employees can access the internet, emails and social networking sites via their own personal devices so this policy also covers the employee's use of their personal mobile device / smartphone or any other means of electronic interaction when conducting Council business.

2.4 Information or data which is sensitive, council confidential, or personal must be stored on secure systems and, if appropriate, be encrypted. For guidelines on data encryption, please refer to the **Data Encryption & Portable Media Policy**.
(<http://www.swansea.gov.uk/staffnet/policysearch>)

2.5 For security and network maintenance purposes, authorised individuals within CCOS may monitor equipment, systems and network traffic at any time, in line with CCOS's Audit Policy.

2.6 Responsibility for the implementation, monitoring and development of this policy lies with the Head of Human Resources. Day-to-day operation of the policy is the responsibility of nominated officers who will ensure that this policy is adhered to.

3.0 Security information

3.1 Information contained on corporate systems is often confidential, depending on the nature of the data. Staff should take all necessary steps to prevent unauthorized access to this information. Further details can be found on our protecting information webpages.
(<http://www.swansea.gov.uk/staffnet/protectinginformation>)

3.2 Staff must keep passwords secure and not share accounts. For guidelines on passwords, please refer to the **CCOS Password Policy**.
(<http://www.swansea.gov.uk/staffnet/policysearch>)

3.3 All PCs, laptops, workstations and other devices are secured with a password-protected screensaver with the automatic activation feature set at 10 minutes. However, staff should lock their device as soon as they leave them unattended using the "Windows" and "L" keys together.

3.4 Mobile computing is increasing and the risk of loss or theft has increased accordingly. Unencrypted laptops can allow unauthorised access to the data contained on them, and so must be protected. It is the user's responsibility to ensure that their device has been installed with the encryption software provided by the ICT Service prior to using them for Council business. For the avoidance of doubt, this also includes portable data storage systems such as USB sticks and external hard drives.

3.5 Employees using a CCOS email address should not post to newsgroups unless posting is authorised and in the course of business duties.

3.6 All devices used by the employee that are connected to the CCOS Internet/Intranet, whether owned by the employee or CCOS, shall have approved virus-scanning software with a current virus database. Employees should not open e-mail attachments received from unknown senders, as they may contain viruses, email bombs, or Trojan horse code. January 2016

4.0 Using the internet, email, instant messaging, video conferencing and skype for business

4.1 The Council reserves the right to monitor internet, email, instant messaging, video conferencing and Skype for Business usage. This will include access to user email accounts when necessary.

4.2 Staff should not use the business facilities for internet, email, instant messaging, video conferencing and skype for personal use unless it is used:

- ☐ for work related purposes such as research whilst studying for exams;
- ☐ for purposes of Helping Hands;
- ☐ outside work time, i.e. before or after work or during lunchtime.

4.3 Occasional reasonable use for private emails will be allowed subject to the prior consent of the employee's line manager who will keep a written record of the authorisation - an email exchange will suffice.

4.4 Use of email facility for personal incoming emails is discouraged, although the Council accepts this may be beyond the employee's control. However, if an employee then forwards an inappropriate email, this may be a disciplinary matter.

4.5 Email Content Filtering

The Council uses an externally hosted email filtering service which prevents the sending and receiving of emails which contain:

- ☐ known and suspected virus infections;
- ☐ keywords, including profane and racist vocabulary;
- ☐ attachments whose contents can't be scanned (e.g. encrypted);
- ☐ emails from known SPAM mail originators.

4.5.1 Any mail analysed and found to be in any of the above categories will be blocked. Emails containing known viruses or from known spam sites will be deleted, whilst suspect emails containing profane language and suspect content will be quarantined on the mail server and an email sent to the recipient.

4.5.2 The recipient is responsible for forwarding an email to the ICT Service Desk asking for the email to be released. It should be stressed that users should exercise care when opening these emails, even though all potential threats should have been removed. Note also that, to protect Council email addresses being confirmed or denied and being used by potential scammers, no notification will be given to the sender of the email that it has been blocked.

4.5.3 However, it should be noted that the filtering service is not guaranteed to prevent offensive content, such as inappropriate pictures, being sent to the recipient, and care should be exercised when opening any attachment.

4.5.4 In the event of receiving an inappropriate mail, it should be reported to your line manager, who can take advice from the ICT service desk as to the best course of action.

4.6 Monitoring of Use

4.6.1 All information processed on the Council's system is the property of CCoS and may be accessed or monitored by the Council. Should the need arise, a record of sites visited can be accessed by line managers upon request.

4.6.2 The CCoS reserves the right to monitor staff use of the Internet and email on the Council's systems, including private use to ensure lawful use in accordance with this policy. January 2016

4.6.3 Internet and email monitoring will be carried out only so far as to ensure proper use of the facility, and in particular to stop inappropriate or unlawful use such as sending harassing or defamatory messages to others, or to prevent its use in improper or criminal activities.

4.6.4 Should you personally receive any material which falls into the categories discussed above, or accidentally visit a site that would be deemed unsuitable, make a note of the time and date then contact your line manager who will take the necessary action as advised by HR&OD.

4.6.5 All employees should report possible misuse to their line manager.

4.7 Unacceptable use

4.7.1 The Internet and email facility should not be used for transmitting or receiving material which is:

- ☐ Illegal, obscene, offensive, fraudulent etc.;
- ☐ Discriminatory (as defined by the Equality Act);
- ☐ Defamatory – including libellous and slanderous comments;
- ☐ An intrusion into other people's privacy, or which may be construed as harassing them;
- ☐ In breach of Copyright (NOTE: it is illegal to download or copy material without prior permission of the owner; Furthermore, Copyright in material exists automatically, and no statement to this effect is required);
- ☐ In contravention of the Data Protection Act (using personal data for unauthorised purpose);
- ☐ Confidential information

4.7.2 Do not use the Internet or e-mail facility for:

- ☐ Chain letters;
- ☐ Private business use or personal advertisements;
- ☐ Chat lines or playing games;
- ☐ On-line betting or gambling;
- ☐ Newsgroups, Bulletin Boards, Mailing Lists other than for work purposes, unless in agreement with your line manager – any line manager giving permission for this will need to keep a record of such subscriptions. These are areas where names and addresses are made available to a wider audience and as such could result in junk mail (spam) causing overloading of mailboxes and wasted time;
- ☐ Downloading files, Shareware or Freeware – you may not be aware of the correct licensing issues; in addition, you could introduce viruses into the organisation – it is important that you stick to safe sites. CCOS staff are reminded that all software must be installed by the ICT service only;
- ☐ Downloading/streaming of video/audio programs as this can cause network congestion – it should only be done with the authorisation of your line manager and outside general office time when necessary;
- ☐ Purchasing on-line, other than for work purposes, and then only in accordance with the Council's e-commerce and general procurement policy.

4.7.3 Caution:

- ☐ Pictures, jokes, 'amusing stories' or inappropriate language – these could be interpreted by somebody as discriminatory, and another person's perception may not be the same as yours. Be aware that any such items could be potentially offensive and may lead to legal action if construed as defamatory or amounting to harassment;
- ☐ E-mail is not private – it can be copied, forwarded. You may delete it, but it could still reside somewhere and may be later accessed and read;

January 2016

- ☐ Computer Security – it is your responsibility to ensure security. You must keep your password confidential, do not allow unauthorised use of your PC – you will be held responsible for all mail items using your ID or for any work carried out using your password; do not access other people's mailboxes without permission. When

investigating misuse of the e-mail and internet facilities, special consideration will be given to employees who use a shared facility;

- ☐ Think when submitting personal/company details – it could result in unwanted junk mail, or possibly facilitate fraud against you or the Council;
- ☐ E-mail – Any correspondence entered into can be classed as a contract and could be used in any legal action against you or the Council;
- ☐ Attachments – could contain a virus, therefore take care when opening from an unknown source.

DO NOT access email of any other employee unless specifically authorised.

DO NOT send emails from another employee's computer unless specifically authorised.

4.8 Prohibited activities

The following activities are strictly prohibited, with no exceptions:

- ☐ Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CCoS;
- ☐ Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which CCoS or the end user does not have an active license is strictly prohibited;
- ☐ Exporting software, technical information, encryption software or technology, in violation of international or national export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- ☐ The introduction of malicious programs into the network or server (e.g. viruses, worms, Trojan horses, email bombs, etc.);
- ☐ Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home;
- ☐ Allowing any person not employed by the council, or who is not an elected member, access to or use of council equipment, unless the council have given authorisation for the action;
- ☐ Using a CCoS computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or workplace laws;
- ☐ Making fraudulent offers of products, items, or services originating from any CCoS account;
- ☐ Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;

NOTE: Any possible or actual security breaches must be reported to the Council's Security Officer via infosec@swansea.gov.uk;

- ☐ Port scanning or security scanning is expressly prohibited unless prior notification to CCoS is made;
- ☐ Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty;
- ☐ Circumventing user authentication or security of any host, network or account;
- ☐ Interfering with or denying service to any user (e.g. denial of service attack).
- ☐ Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet;
- ☐ Providing information about, or lists of, CCoS employees to parties outside CCoS;

- ☐ Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam);
- ☐ Any form of harassment via email whether through language, frequency, or size of messages;
- ☐ Unauthorized use, or forging, of email header information;
- ☐ Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies;
- ☐ Creating or forwarding "chain letters", or other "pyramid" schemes of any type;
- ☐ Use of unsolicited email originating from within CCoS's networks of other Internet service providers on behalf of, or to advertise, any service hosted by CCoS or connected via CCoS's network;
- ☐ Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Social Media and Networking

5.1 Staff and members are not given general access to social networking sites from CCoS networks. 'Social media' is the term commonly given to websites and online tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests.

5.2 Staff are only granted access to social media for specific business reasons in a work-related professional capacity and further information can be found in the **Social Media Usage Guidance document**. Staff must always use social media / social networking in line with the principles of this policy during working hours or otherwise.
<http://www.swansea.gov.uk/staffnet/ictsystemsguidelines>

5.3 Outside CCoS, staff can freely access social media sites but this must be handled in a sensible and considered way so that neither the individual(s) involved nor the Council is put at potential risk of embarrassment, loss, disciplinary action or criminal proceedings.

5.4 Staff should never publish or disclose any confidential information or information about the Council which is not already in the public arena. Staff must ensure that online activities do not interfere with their job, colleagues or commitments to customers. Staff should not post negative comments about their work, the Council or their colleagues.

5.5 Staff should not post any comments about the Council that do not represent the views of the Council. It is possible that outside activities could lead to complaints of harassment or bullying even though they are not committed in the workplace.

5.6 Staff should not use social media or networking sites to befriend service users or attack or abuse colleagues, customers or suppliers.

5.7 Any abusive or inappropriate comments whether made to or about the Council, colleagues, customers or suppliers will not be tolerated and may lead to legal liability as well as disciplinary action including dismissal.

5.8 Accessing social networking from personal equipment.

Employees should not ordinarily access any form of social networking, email or internet site via their mobile or otherwise for personal use during working time. Any employee found to be doing this excessively may be subject to disciplinary proceedings.

6.0 Telephones and fax machines

6.1 Telephones and fax machines are provided for staff to undertake CCoS duties. They should only be used for personal purposes if the matter is considered urgent. The line manager's permission should always be sought first and calls recorded.

.0 Mobile phones

7.1 This policy will apply to all Council employees (permanent and temporary) and contractors using or who are provided with a mobile phone to assist them in the performance of their duties or through personal choice.

7.2 The policy is designed to ensure that there are clear internal arrangements for the effective management of mobile phones. Line managers are responsible for ensuring that their staff are aware of the location of this policy. In addition, line managers are responsible for keeping staff up to date about any changes within the policy.

7.3 The policy ensures that Health & Safety issues are identified in relation to the use of mobile phones, and ensures compliance with legislation on mobile phones and driving.

7.4 This policy sits in support of local level arrangements and procedures for lone working. These will in all instances be to a standard compliant with both the requirements of the Corporate Health & Safety and Corporate Lone Working Policies.

7.5 The policy establishes the responsibilities of employees of the Council in regard to the issue and use of Council mobile phones. All staff that use a Council mobile phone are obliged to adhere to this Policy. Failure to do so may result in disciplinary action.

7.6 Criteria for Issue of a Council Mobile Phone

7.6.1 Mobile telephones will only be available to staff who have the approval of their line manager, and authorisation of the appropriate Head of Service. An employee will be eligible to have a mobile phone if it is deemed necessary to their position, and they meet any one of the following criteria;

- If the employee's duties require them to spend a substantial amount of time out of the office on work related duties (substantial is defined as an average of more than 50% of their working day);
- Staff for whom it is necessary to make essential work related calls off site, as part of their normal course of work;
- Staff who are required to be contactable in an emergency situation, when working off-site;
- Staff who are on call after normal business hours;
- Staff identified through the risk assessment procedure;

7.7 Pool phones

7.7.1 Mobile telephones may be issued on an individual or on a shared basis i.e. shared phones for people on call. In all cases it is the line manager's responsibility to determine which officers will be part of a shared resource pool, and how this will operate within their area of control.

-

7.8 Purchase of Mobile Phones

7.8.1 The purchase of mobile telephones must be in compliance with the Council's Procurement Policy and co-ordinated by the ICT Delivery Team.

<http://www.swansea.gov.uk/staffnet/ictdeliveryteam>

7.8.2 A mobile phone request can be initiated via the Council's self-service system AssystNet and must be completed via an authorised user.

7.8.3 Any requests for a specific model of mobile phone outside the standard phone issued by the Council will be dependent on the user demonstrating the business requirement and this is likely to incur additional charges to the user.

7.8.4 All costs for the purchase and use of mobile phones will be charged to the appropriate directorate budget. It is the responsibility of each Head of Service to ensure that adequate provision is made in the annual estimates to cover the cost of all mobile phones issued within their directorate.

7.8.5 Where a phone contract is renewed and a new upgraded mobile phone is provided, the current handset that is being replaced must be returned to the ICT Delivery Team.

7.9 Rules of Mobile Phone usage and best practice

7.9.1 Council mobile phones must be on at all times during business or call out hours, except when driving. Please refer to 7.14.2 for further guidance on driving and the use of mobile phones.

7.9.2 Mobile phones should be switched off during meetings, lectures, seminars, training courses etc. other than in very exceptional circumstances where it is necessary to take an urgent call. In these circumstances it is courteous to alert colleagues to the fact that an urgent call is expected and where possible, the phone should be kept on 'silent'.

7.9.3 Confidential information must not be discussed in open areas or inappropriate locations. Many departments/buildings (e.g. hospitals), have local rules regarding the use of mobile phones and these must always be respected. Discretion should be used at all times.

7.9.4 The phone must be returned to their line manager for any periods of extended leave, including maternity.

7.10 Private Use of Mobile Phones

7.10.1 Council issued phones are intended primarily for CCoS use. The current mobile phone tariff is an all-inclusive package for calls and texts, with the exception of some specific numbers as detailed on the mobile phone intranet page.

(<http://www.swansea.gov.uk/staffnet/mobilephoneorders>).

7.10.2 A data package will be automatically added to the standard tariff for all smartphones i.e. 'essential business users' at a cost detailed on the webpages. Any excessive use of data as a result of personal use will incur additional charges to the user. All bills for any chargeable calls incurred must be settled promptly. Failure to do so may result in this benefit being withdrawn.

7.10.3 Line managers and supervisors will monitor usage of Council mobile phones for both private and business use. Private use is at the line manager's discretion, however should be kept to a minimum and in cases of emergency. January 2016

7.11 Lost or Broken Mobile Phones

7.11.1 The Council expects all employees, who have been allocated mobile phones, to take the utmost care and responsibility for them. If a phone is lost or stolen, it should be reported immediately to your line manager and also the ICT delivery team in order to minimise the financial exposure. The phone can then be securely wiped of any Council data. (<http://www.swansea.gov.uk/staffnet/ictdeliveryteam>).

7.11.2 If a phone is broken or faulty, please report the fault to the ICT Service Desk and return the faulty handset to the ICT delivery team. A temporary phone may be issued until repair can be affected. If the phone cannot be repaired, a request for a replacement phone will be required.

7.11.3 Depending on the circumstances in which the phone was lost or broken, the Council will be responsible for replacing the phone. However if carelessness on the part of the employee can be shown as the cause of the loss, the employee will be required to meet the replacement cost.

7.12 Termination of Employment

7.12.1 On termination of employment, the employee must remove any Council data on the mobile phone and return it to the ICT delivery team, unless the line manager has authorised a transfer to a new user using the appropriate notification via AssystNet. Any accessories supplied by the organisation for use with the mobile phone must also be returned.

7.12.2 Employees who transfer to other departments within the Council and are authorised to have continued use of a Council mobile phone must inform the ICT delivery team and they will inform the provider of the change in account details.

7.13 Use of Mobile Phones whilst travelling abroad

7.13.1 All CCoS mobile phones and devices will have 'global roaming' disabled by default, meaning that they will not be able to make and receive calls whilst abroad. If global roaming is required by a user, then it should be requested by email, with authorisation by the line manager to the ICT delivery team at least one week prior to the date of departure and confirmation of activation will be confirmed. Be aware that changes to account settings cannot be made once the device is outside the UK.

7.13.2 Whilst travelling abroad and with global roaming enabled you have the ability, should you choose, to select which network to operate on. Your phone has a default setting that enables it to select the most appropriate network based on agreements with the Council's service providers and radio signal quality. It will constantly monitor these factors and will change networks when appropriate. You do not need to change any network settings.

7.13.3 Care must be taken when roaming to avoid high call costs. When you are roaming you pay for any calls that you receive as well as for calls that you make. Roaming call charges, for both 'made calls', 'received calls' and access to voicemail are very expensive and further guidance can be obtained from the ICT Delivery Team. (<http://www.swansea.gov.uk/staffnet/ictdeliveryteam>).

7.13.4 Text messaging is more expensive when roaming and usage should be kept to a minimum.

7.14. Health and Safety aspects of Mobile Phone use

7.14.1 The Council's Health & Safety team provides advice and guidance on the use of mobile devices in conjunction with the appropriate legislation. Further details can be found on their website.

(<http://www.swansea.gov.uk/staffnet/healthandsafetyguidancesearch>) January 2016

7.14.2 Driving and the Use of Mobile Phones. The Department for Transport has warned that Employers should issue clear guidance about the use of mobile phones and ensure that users are fully aware of the circumstances. In particular, the following points should be noted:

- That it is illegal to use a hand-held mobile phone when driving.
- To keep any mobile phone switched off when driving and use voicemail, a message service or call diversion so that messages can be left when the phone is switched off.
- That a mobile phone should only be used after the driver has stopped in a safe place. (Never stop on the hard shoulder of a motorway except in an emergency).
- Avoid taking calls on a hands-free phone, but if the driver must, they should say that they are driving and end the conversation quickly.
- Those drivers' may use a mobile phone when driving to call for assistance in an emergency. (On a motorway it is best to use a roadside emergency telephone, as the emergency services will be able to locate you easily).

7.14.3 The City & County of Swansea does not approve of any use of mobile phones whilst driving. This includes making and receiving calls and text messages even if you have a car kit. Do not make or receive calls whilst driving!

7.14.4 Drivers are legally obligated to have proper control of their vehicle at all times. The existing maximum penalty for unsafe driving can be an unlimited fine, up to two years in prison, between 3 and 9 penalty points, a discretionary disqualification and an extended re-test.

IF YOU ARE DISQUALIFIED FROM DRIVING, YOUR JOB AND POSITION WITHIN THE LOCAL AUTHORITY MAY BE AFFECTED.

7.14.5 Guidance may be issued to mobile phone users from time to time regarding health & safety in relation to their use, (i.e. Legislation on mobile phones and driving guidance notes, and must be observed at all times).

7.14.6 Staff must ensure that, when they carry a Council mobile phone, they have included in the contacts the number of their line manager and emergency services.

7.14.7 Where identified through risk assessment as a control measure, managers must ensure that a mobile phone is provided. The details of this risk assessment and all control measures must be communicated to the employee. This would include any local level arrangements for lone working and emergencies (i.e. starting and finishing on-site).

7.14.8 Employees are responsible for ensuring that any issued mobile phone is charged and in working order at all times, reporting any defect immediately to their line manager.

7.15 Mobile Phone Security - Passwords

7.15.1 Smartphone devices provide access to the user's contacts, email and calendar which may contain confidential, and sometimes, personal information. Due to its small size a Smartphone is likely to be carried into places a laptop would not be, and therefore the user must ensure that the device is physically secure at all times. This should also include any personal phones which access Council data.

7.15.2 Each device is provided with a password/ PIN facility securing access which should be enabled at all times as a minimum security measure. If a device is lost, this must be reported to ICT delivery team immediately. January 2016

7.16 Publication of mobile phone numbers

7.16.1 Council mobile phone numbers may be published in any of the following locations:

- ☐ Business Cards
- ☐ Email auto-signatures
- ☐ Internal Local Authority telephone directories
- ☐ Local Authority, school and department websites

7.16.2 In certain circumstances a mobile phone user may not want their number published for legitimate reasons. This is decided on a case-by-case basis.

7.17 Mobile phone monitoring and charges

7.17.1 All charges and other costs associated with the purchase, connection, operation and maintenance of mobile devices are the responsibility of the users cost centre.

7.17.2 The Cost Centre Manager is responsible for monitoring the usage in the following areas:

- ☐ Out of hours calls
- ☐ Private calls
- ☐ Long distance calls including international and roaming costs
- ☐ High cost calls
- ☐ Premium rate numbers
- ☐ Frequently dialled numbers
- ☐ Text Messaging
- ☐ Premium Text Messages and services
- ☐ Data Use

7.17.3 Where personal use is identified, the CCoS reserve the right to pass on all or any part of these costs to the end user. Any such charges may be deducted from the users' salary payment after notification from the relevant Cost Centre Manager.

7.17.4 The CCoS reserve the right to place restrictions on mobile devices including but not limited to restricted dialling, removal of text messaging capabilities or other services.

8.0 Reference Documentation

8.1 This Policy should be read in conjunction with the following legislation, regulations and Council policies:

- Data Encryption & Portable Media Policy
- CCOS Password Policy
- H&S Laptop and mobile devices guidance
- Social Media Usage guidance
- Management of Health & Safety at Work (NI) Regulations 2000
- CCoS Lone Worker Risk Assessments
- The Motor Vehicles (Construction and Use) Regulations (NI) 1999 and Road Traffic (NI) Order 1999
- Report "The Risk of Using a Mobile Phone While Driving" 2002 (The Royal Society for the Prevention of Accidents)

Version Number

3.0

Details of Change

Combined with the current internet and email policy and the new internet, social networking and telephone policy

Date

January 2016