Email and the internet are key tools. The use of department information and communication technology (ICT) facilities is governed by the department and Government policies. These policies are in place to protect department information and ICT assets from a range of threats including loss, corruption, disclosure, theft and interruption of services.

Purpose	ICT facilities are provided to support the department's role as a provider of public children's services and schooling, and the administrative functions and technical services that underpin this provision. All staff are required to familiarise themselves with ICT policies. In addition, all users of the department's ICT facilities have read and signed an acceptable use agreement.

Users of department ICT facilities must:

1. Ensure the PLINK Cyber Security Training Course has been completed.
2. Read and understand the Department for Education's ICT cyber security standard and observe and be bound by its conditions at all times.
3. Use department ICT facilities in an appropriate and professional manner according to the **Code of Ethics for the South Australian Public Sector** published by the Commissioner for Public Employment.
4. The Practical guide for the use of email and the internet guideline is a recommended course of action to ensure that all staff use the resources of the email and internet systems in a consistent and sustainable manner. It is based on recommended best practice.
5. Follow the directions of ICT Service Desk relating to their use of department ICT facilities.
6. The department ICT facilities must not be used for the access, transmission , retrieval, storage or display of:
   - sexually explicit material
   - hate speech or offensive material
   - material regarding illicit drugs or violence
   - material regarding criminal skills and/or illegal activities
   - material of a defamatory, discriminatory or harassing nature.

   This includes accessing any sites or forums that deal with these materials. The only exception is if the material forms part of a legitimate educational inquiry and approval has been gained from the principal.
7. The department reserves the right to monitor usage of the department internet and email services and facilities.
8. User agreements must be signed before a user is given access to systems. For staff, the following is recommended for periodically re-signing agreements:
   - if any major changes are made to the agreement
   - if the staff member has been involved with any disciplinary action involving their unacceptable use of ICT assets

Personal use

The department recognises that, consistent with the provision of a family friendly work environment and the promotion of the department as a learning organisation, some personal use is reasonable. However, it must also be recognised that use of the department's internet and email facilities is not free, and you are required to use all resources, including these facilities, efficiently and effectively for public benefit.

Therefore limited personal use of email and the internet is permitted as long as:

- there is no significant additional cost to the department
- it does not interfere with the user's work or the activities of others
- there is no effect on the efficiency of the department's network
- use is not classified as inappropriate or restricted.

Non-compliance with the department policies may result in disciplinary proceedings against an employee or others provided with access to the department ICT facilities. Furthermore, any material found that may be related to child pornography or paedophilia will be referred to the SA Police.

Electronic mail access and use

Email records, either hard copy or electronically stored, which the department has access to, are documents which may be subject to a freedom of information application under the South Australian Freedom of Information Act 1991 and may have to be released whether or not the individual who created them wishes them to be.

All email transmitted, received and stored remain the property of the department.

Staff must add a disclaimer to email where their expressed views are not necessarily those of the department.

Staff must at all times observe copyright, and licensing laws when including copyrighted material, in their use of the department email facilities.

Primary usage

Email must be primarily used for the department related business purposes, e.g. communications related to the department business, authorised personal development and activities related to a person's duties.

Unacceptable usage

The department's reputation as a professional organisation must not be jeopardised by improper use or conduct via email. Usage that causes interference or disruption to other email users will not be tolerated.

Unacceptable usage includes, but is not limited to:

- distribution of unsolicited advertising
- distribution of 'chain letters'
- propagation of any form of malicious software or code (malware, viruses, phishing)
- distribution of offensive material, including jokes or images
- use causing harassment, defamation or offence to others
- activity which involves religious or political lobbying
- excessive non-department business use
- distribution for personal financial gain.

Representation

Communications using the department ICT facilities should not give the impression that you are representing, giving opinions, or otherwise making statements on behalf of the department, unless appropriately authorised (explicitly or implicitly) to do so. To avoid confusion, it is recommended that a disclaimer be included on all your emails which states:

> *'This email and any attachments may contain confidential information. If you are not the intended recipient any use, disclosure or reproduction of the contents is unauthorised. If you have received this email in error please notify the sender by return email. This email and any attachments should be scanned to detect any viruses and no liability for loss or damage resulting from the use of any attached file is accepted.*
>
> *Unless otherwise stated, the contents of this message contain the opinions of the writer, and not the policy of the department or the Government of South Australia.'*

You can simply achieve this by configuring your email client software (ie Microsoft Outlook) to automatically include this on your email's 'signature'.

Internet access and use

Access to the internet is to be used primarily for department related business purposes, e.g. communications related to department business, authorised professional development and activities related to a person's duties.

Interference or disruption to other networks or shared-system users, services or equipment will not be tolerated.

Unacceptable usage includes but is not limited to:

- visiting inappropriate internet sites concerned with pornography and downloading materials that are pornographic, or storing or transmitting any such material
- downloading and/or distributing copyrighted material without proper authority
- unreasonable level of use of the department's ICT facilities in pursuit of non-work-related personal interests
- playing or downloading computer games
- participating in chat rooms or the use of messenger or chat programs for non- business related activities

Internet access and use *continued*

- access to streamed broadcasts eg movies and radio stations. Access to streamed broadcasts via the internet will only be considered appropriate when used for professional development or upon the authorisation of line managers
- conducting regular personal correspondence
- publishing or circulating a journal or newsletter without authorisation.
- distribution of unsolicited spam, advertising or commercial electronic messages
- distribution of electronic 'chain letters'
- accessing of malicious, offensive or harassing material
- distribution of offensive or harassing material
- propagation of any form of malicious software (viruses, malware, etc)
- use of the network to make unauthorised entry into other information systems, communications devices or resources.
- postings for non-business related reasons
- use for personal financial gain
- use of non-approved file sharing technologies
- use for religious or political lobbying
- downloading or sharing of non-business material.

The department reserves the right to record and monitor Internet usage, for the purposes of managing system performance, monitoring compliance with policies, or as part of disciplinary or other investigations.

Mobile communication devices security

Mobile communication devices are defined as devices that can store, send and receive communications (voice, data, text and video) while the device is not physically attached to a network. Mobile communication devices include mobile telephones, tablet devices using wireless/mobile telecommunication technology (eg iPad, Android, Windows devices etc), smart phone devices and laptops/notebooks with wireless/mobile telecommunication connectivity.

When using mobile communication devices, special care must be taken to ensure that information is not compromised through use of the equipment outside of the Department for Education environment.

- Only a copy of information should be used on the device.
- Devices must be password protected with auto-lock where possible
- Never leave mobile communication devices unattended in a public place, car (even if locked), or in an unlocked house or office.
- Department for Education mobile communication devices must not be used by staff members' family, friends or non-Department for Education personnel.
- Department for Education mobile communication devices must not have unauthorised applications or software installed.

Information stored on a mobile communication device that is sensitive, such as information that is personally identifiable, commercial, or that may cause reputation damage to the department if leaked/lost, requires the following extra precautions:

- Password protection of the specific file or system.
- Encryption of the information (including backups).
- If connecting to a Department for Education network remotely, ensure information is encrypted when sending or receiving.

References:	*Acceptable use policies for schools, preschools and children's services' sites standard* *Code of Ethics for the South Australian public sector* *Practical guide for the use of email and the internet guideline* *ICT Cyber security standard* *ICT security risk assessment procedure* *Mobile communication devices procedure* *PLINK Cyber Security Training Course*