The Distance Education Centre, Victoria
‘Flexible Learning for All’

*Digital Education Revolution*

*Acceptable Use Policy and Agreement*

One copy of this agreement must be completed by each Student participating in the program.
This form must be completed by all DER recipients

DECV
COMPUTER / INTERNET ACCESS
STUDENT CODE OF CONDUCT

Student Name: ______________________________________________

Year Level: ______    DECV Student Number ________________

I, the student whose name appears above, agree to the following:

1. I acknowledge that this computer does not have Internet filtering software. Therefore, I
   will only access appropriate software, information and send messages that are relevant
   to the work I am undertaking. I understand I can request an Internet filter to be loaded on
   this computer if required as a student, by a parent / guardian or by teachers.

2. I acknowledge that as a student, I do not have in my possession any other DER funded
   computing device from another school.

3. I acknowledge that I will be expected to reimburse the school for the cost of any damage
   or theft that I am responsible for.

4. I will not attempt to load, corrupt or alter any files or applications on the school’s
   computer systems / network or resources.

5. I will not deliberately access pornographic, violent, drug related or socially unacceptable
   material via the Internet, or by any other means. If pornographic or socially unacceptable
   material is accidentally located, I will inform my teacher immediately.

6. I will follow sensible precautions when using my username and password: I will keep my
   password secret; I will only log on to a computer with my own user name and password,
   and will always log off when I have finished with a computer. I realise that I will be
   responsible for activities that occur with my username and password.

7. I will respect the e-mail and password privacy of my fellow students.

8. I will ensure that any e-mail, chat or other communication that I send out, shows that I
   am a positive ambassador for the DECV, and will not contain any inappropriate or
   offensive content. Material cannot be transmitted that violates state, federal or
   international regulations – including but not limited to: copyrighted material, threatening,
   harassing or obscene material, pornographic material or material protected by trade
   secret.

Student Name (Please print) ____________________________

Parent/Guardian Name (Please print) ____________________________

Signature ____________________________    Signature: ____________________________

Date:     /    / 2012    Date:     /    / 2012
Please retain for your information

DEECD ACCEPTABLE USE POLICY
FOR
INTERNET, EMAIL AND OTHER ELECTRONIC COMMUNICATIONS

1. Scope

1.1. This policy applies to the users of DEECD network or DEECD equipment, which includes but is not limited to all staff, contractors, casuals, temporaries and volunteers of DEECD, all schools, regions and school councils.

1.2. Use of the DEECD network includes transmissions to or through the DEECD network by a party described in paragraph 1.1.

1.3. This policy governs the use of all electronic communications (excluding telephones), and includes but is not limited to:

- Publishing and browsing on the internet (including Intranet and Extranet) and Electronic mail (‘Email’),
- Electronic bulletin/notice boards,
- Electronic discussion/news groups,
- File transfer,
- Video conferencing,
- Streaming media,
- Instant-messaging and ‘Chat’ facilities.

All of which are referred to in this document as “Electronic Communications”

1.4. Any reference in this policy to an Act, law, Code of Conduct or other document includes a reference to the Act, law or document as amended from time to time.

1.5. In this policy –

   (i) an “Authorised Person” means a person authorised by the Secretary to the Department of Education and Early Childhood Development.
   (ii) Personal Information is information or opinion about a person whose identity is apparent or can reasonably be ascertained from the information or opinion.
   (iii) Sensitive information is information or opinion about a person’s health, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, or criminal record.

2. Purpose

2.1. The purpose of Electronic Communications within DEECD is to conduct the business and functions of DEECD.

2.2. The purpose of this Policy is to ensure that Electronic Communications are properly and efficiently used, and that the Department is protected from problems such as error, fraud, defamation, breach of copyright, unlawful discrimination, illegal activity, privacy violations and service interruptions.
3. **Rationale**

3.1. The use of Electronic Communications at DEECD is a privilege, and like any other privilege, carries with it responsibilities.

3.2. Publishing, accessing information and communicating electronically can be cost-effective, timely and efficient. It is essential that use of this valuable resource be managed to ensure that it is used in an appropriate manner.

3.3. The process by which DEECD seeks to manage staff use of Electronic Communications is through the development and implementation of this Policy. The Policy provides specific instructions, which must be followed whenever using Electronic Communications.

4. **Responsibility**

4.1. It is the responsibility of General Managers, Managers, and Principals to ensure that the persons to whom this Policy applies are aware of this Policy. This should include, but is not limited to –
   (a) Providing a copy of the Policy,
   (b) Regular and timely reminders of the need for compliance with the Policy,
   (c) Providing updates or developments of the Policy,
   to those affected by the Policy.

4.2. It is the responsibility of individuals to abide by the Policy.

5. **Non – Compliance**

5.1. Non-compliance with this Policy will be regarded as a serious matter and appropriate action will be taken when a breach of the policy is identified.

5.2. Any failure to abide by this Policy may result in disciplinary action including revoking or restricting any right to use Electronic Communications, cautioning, or, in appropriate circumstances, may lead to more serious disciplinary action including termination of employment.

5.3. Non-compliance with this Policy may pose a threat to the security of the DEECD network, the privacy of staff and other persons and may expose the users of the system or other persons to legal liability.

6. **Business Purposes**

6.1. DEECD Electronic communications network is primarily a business tool to be used for DEECD purposes.

6.2. Electronic Communications must –
   (a) Only be used for DEECD purposes, or where authorised or required by law, or with the express permission of an Authorised Person, and
   (b) Be used like other business communications and comply with any codes of conduct which apply to the user, such as the Code of Conduct for the Victorian Public Sector, and Teaching Service Orders.

6.3. Users of the DEECD network may use Electronic Communications for limited personal use as long as this does not interfere with their role within DEECD, is reasonable and not excessive. Unreasonable or excessive personal usage
constitutes is a failure to abide by this policy and may result in the consequences set out in paragraph 5.

6.4. Subject to limited personal use in accordance with clause 6.3, electronic communications must generally not be used to conduct private business or private commercial transactions, gamble, or carry out research into non-work related topics.

6.5. Subscribing to list servers (LISTSERVS), mailing lists and other like services must be for DEECD purposes or professional development reasons only.

6.6. On-line conferences, discussion groups or other like services must be relevant and used for DEECD purposes or professional development activities. Such interaction requires that internet etiquette should be observed along with current societal standards for respect and fairness.

6.7. Obtaining unauthorised access to electronic files of others, or to Email or other Electronic Communications of others, is not permitted.

6.8. Large downloads or transmissions should be minimised to ensure the performance of Electronic Communications of other users are not adversely affected.

7. Department Property

7.1. DEECD is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through DEECD’s network.

7.2. Electronic Communications created, sent or received by the users referred to in paragraph 1.1 are the property of DEECD, and may be accessed as records of evidence in the case of an investigation. Electronic Communications may also be subject to discovery in litigation and criminal investigations. For example, all information produced on computer, including Emails, may be accessible under the Freedom of Information Act. Email messages can, and have been, retrieved from backup systems and organisations, their employees and the authors of email have been held liable for Email messages that have been sent.

8. Monitoring

8.1. Electronic Communications will be treated as DEECD related and may be monitored by Authorised Persons.

8.2. It is not DEECD’s policy to regularly monitor Electronic Communications. However, from time to time Authorised Persons may examine the records of Electronic Communications including for operational, maintenance, compliance, auditing, security or investigative purposes. For example, random monitoring may occur of web sites visited, the contents of Email may be required by law to be disclosed or DEECD may investigate a complaint arising from the use of Email.

8.3. Electronic Communications are provided to you on conditions that you agree to monitoring in accordance with this Policy. Your use of Electronic Communications constitutes your consent to monitoring in accordance with this Policy.

9. Defamation

9.1. Electronic Communications must not be used to send material that defames an individual, organisation, association, company or business. The consequences of a defamatory comment may be severe and give rise to personal and/or DEECD liability. Electronic Communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and extremely widespread.
9.2. All users of Electronic Communications must ensure they are familiar with the following publications issued by DEECD.

10. Copyright Infringement

10.1. The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, text and downloaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing copyright material by electronic means, may give rise to personal and/or DEECD liability despite the belief that the use of such material was permitted.

10.2. DEECD supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.

10.3. All users of Electronic Communications must ensure they are familiar with the following publications issued by DEECD

10.3.1. Guidelines on Copyright and Trademark Management; and

10.3.2. Copyright for Schools

11. Illegal/and offensive material

11.1. Electronic Communications must not be used in any manner contrary to law or likely to contravene the law. Any offender will be referred to the police or other relevant authority and their employment may be terminated.

11.2. Offensive material must not be accessed or distributed in any manner contrary to law. This includes defamatory, racially vilifying, pornographic or unlawfully discriminatory material.

11.3. In particular, DEECD is an institution charged with the safety and education of children, and child pornography is both abhorrent and represents the antithesis of our responsibilities to children. Any offender will be referred to the police and their employment may be terminated.

12. Confidentiality

12.1. Electronic Communication is not a secure means of communication. While every attempt is made to ensure the security of DEECD’s computer network, users must be aware that this security is not guaranteed, particularly when communicated to an external party. The sender should consider the confidentiality of the material they intend to send when choosing the appropriate means of communication.

12.2. Users are required to control the use and release of personal information and restrict access to personal information in order to protect privacy. Collecting, using and disclosing personal information by email may put the privacy of personal information at risk. Personal information and sensitive information should be treated as confidential information. The sender should consider the potential risks of inadvertent or unauthorised disclosure when sending personal information by email. Only the minimum amount of personal information necessary to accomplish the purpose for which it is required should be transferred by email.

13. Viruses

13.1. Electronic Communications are potential delivery systems for computer viruses. All data, programs and files which are downloaded electronically or attached to messages should be run through a virus scan program before being launched, or opened or accessed.
13.2. Viruses have the potential to seriously damage DEECD’s network. Do not open any downloaded files or Emails or attachments that you are not expecting or that look suspicious. In the event that you receive any files that you suspect contain a virus it should be reported immediately to your line manager.

14. Inappropriate content

14.1. The author and/or DEECD may be liable for what is conveyed in electronic communications. Electronic Communications, whether sent internally or externally, must only contain content that is appropriate to a work place environment.

14.2. Electronic Communications must not be used to publish, send or distribute material that is harassing, obscene or threatening, nor may it contain content that may be considered unlawfully discriminatory, offensive or disruptive. This includes sexually oriented messages or images and sexual harassment messages. All users of Electronic Communications should be familiar with ‘Rights and Responsibilities under the Victorian Equal Opportunity Act 1995: training for principals, staff and school councils’

15. Attribution

15.1. There is always a risk of false attribution of Electronics Communications. It is possible that communications may be modified to reflect a false message, sender or recipient. In these instances an individual may be unaware that he or she is communicating with an impostor or receiving fraudulent information. At any stage if a user has a concern with the contents of a message received or the identity of the publisher of the electronic information, action should be taken to verify their identity by other means. If a user believes an electronic Communication has been intercepted or modified, the line manager or principal should be informed.

15.2. Users are accountable for all use of DEECD systems performed with their user-ID. User-ID’s and password must be kept secure and confidential. Active connections are to be terminated when access is no longer required and PCs secured by password when not in use

16. Mass distribution

16.1. The use of Electronic Communications for sending ‘junk mail’, for-profit messages, or chain letters is strictly prohibited.

16.2. Mass Electronic Communications should only be sent in accordance with normal DEECD procedures.
17. Records Management

17.1. Electronic Communications are public records and subject to the provisions of the Public Records Act 1973.
17.2. DEECD record management practices for management of Email messages must comply with the Interim Guidelines for the management of Electronic Mail messages of September 1999 ("The Guidelines"). All users of Email must be familiar with DEECD's 'Recordkeeping Policy and Guidelines, June 1999'.
17.3. Email messages that are routine or of a short term facilitative nature should be deleted when reference ceases, as distinct from ongoing business records such as policy or operational records. For more information see The Guidelines and DEECD checklists for the retention or disposal of electronic messages for DEECD.
17.4. Retention of messages fills up large amounts of storage space on the network and can slow down performance. As few messages as possible should be maintained in a user’s Email account.

18. Disclaimer

All Emails sent externally from DEECD’s EduMail service will automatically have a notice attached to them. The proposed notice is as follows.

18.1. **IMPORTANT** – Any personal or sensitive information herein is intended only for the use of the individual or entity named above. The recipient is responsible for maintaining the privacy of such information herein, and is prohibited from disclosing such information to any other party except in accordance with information privacy legislation. The above obligations are in addition to any obligations of confidentiality that may apply. If received in error, please contact us and delete all copies. Before opening or using attachments, check them for viruses and defects.

18.2. This notice must not be altered or interfered with in any way, except by Authorised Persons. The use of this notice may not necessarily prevent DEECD or the sender of the Email from being held liable for its contents.

19. Complaints

19.1. If you receive an internal or external Electronic Communication which is offensive or inappropriate, raise it with your line manager, or the DEECD Complaints and Investigations Unit, if your line manager is the cause of your complaint.
Rationale

The Distance Education Centre Victoria recognises that student instruction and student learning will change as telecommunications and other new technologies alter the ways in which information may be accessed, communicated and transferred through access to online services.

The DECV also recognises that electronic information research skills are now required as essential knowledge for members of our society and as future employees.

In responding to these changes the DECV actively supports access by students to the widest variety of information resources together with the development, by staff, of appropriate skills to analyse and evaluate such resources.

Access to telecommunications will enable students to explore thousands of libraries, databases, the Internet and bulletin boards while exchanging messages with people throughout the world. The DECV believes that the benefits to students from being able to access and retrieve information from these resources and the opportunities this provides for collaboration, exceed the disadvantages. However, access is a privilege and not a right. Access entails responsibility.

The Role of Students

Students are responsible for good behaviour on school computer networks including the DECV Online Learning Environment. Communications on the information networks are often public in nature and general DECV and DEECD rules for student behaviour, conduct and standards of communications will apply.

Individual users of the DECV computers and networks are responsible for their behaviour and communications over those networks. It is presumed that users will comply with DECV standards and will honour the agreements they have signed.

The Role of Parents

Parents and guardians are ultimately responsible for setting and conveying the standards that their children should follow when using media and information sources.

The DECV expects that these standards will be in accordance with the College Charter, Student Code of Conduct and other general policies of DEECD particularly “Acceptable Use Policy” for Internet, Email and Other Electronic Communications.
The Role of DECV Staff

The DECV expects that staff will incorporate appropriate use of electronic information throughout the curriculum, and that teachers will provide guidance and instruction to students in the appropriate use of such resources.

This will include staff facilitating students accessing information in support of and to enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of students.

The Role of the College

The DECV undertakes a commitment to implement and uphold the DECV Vision and the Online Interactive Learning Communities Vision and to provide resources to facilitate the successful incorporation of access to online services throughout the DECV’s curriculum.

In addition, the DECV will actively support the professional development of all staff to ensure the effective inclusion of telecommunications and other new information technologies into the DECV, its curriculum and its flexible delivery of learning programs.

Student Access

The DECV Online Service and supporting infrastructure is provided for students to access curriculum programs, resources, and services and communicate with teachers and other students.

The use of online services, where made possible by the DECV through student access to telecommunications networks, may lead students to any publicly available information or database in the world. Therefore, prior parental or guardian permission is required for students to be able to access the DECV network or on DEECD/DECV provided equipment.
Student Code of Conduct

Online Access Rules and Network Responsibilities.

The following guidelines apply to all students accessing resources through the DECV’s online network and/or using DECV provided resources.

- Network storage areas where provided will be treated like school lockers.
- Network administrators may access and review files and communications to maintain system integrity and ensure that users are using the system responsibly.
- Users should not expect that files stored on the DECV's computer servers will always be private.

Quite specifically, the following actions are not permitted:

- Sending or displaying offensive messages or pictures.
- Using obscene language.
- Harassing, insulting or attacking others.
- Damaging computers, computer systems or computer networks (for example, by the creation, introduction or spreading of computer viruses, physically abusing hardware, altering source codes or software settings, etc.)
- Violating copyright laws. The legal rights of software producers and network providers, and copyright and license agreements, must be honoured (for example, downloading copyrighted games could result in legal proceedings, resulting in a fine.)
- Using other users’ passwords.
- Trespassing in other’s folders, work or files.
- Employing the network or DECV equipment for commercial purposes or activities by for-profit institutions or organisations, product advertisement or political lobbying is prohibited.
- Using the network to disrupt its use by other individuals or by connecting networks.
- Disrespect of others’ privacy and intellectual property.

1. Transmission of any material in violation of any state, federal or international law and/or regulation is prohibited. This includes, but is not limited to:
   a. copyrighted material, threatening, harassing, or obscene material, pornographic material, or material protected by trade secret.

2. All communication and information accessible via the network should be assumed to be private property. Any sources used in research must be cited and credit given to the author.

3. Security problems must be brought to the immediate attention of a System Administer. The problem must not be demonstrated to other users.

Sanctions.

Sanctions may include the following measures:

- Withdrawal of privileges including on-line access for breaches of online policy.
- Withdrawal from class.
- Recall of DECV provided equipment.

For serious breaches of rules:

- Suspension.
- Expulsion.
- Law enforcement agencies may be involved.