

TALBOT PRIMARY SCHOOL

ICT ACCEPTABLE USE, ICT SECURITY, WIDE AREA NETWORK CONNECTIONS, WIRELESS NETWORKS IN SCHOOLS, NOTEBOOKS PROGRAM POLICIES

Purpose

- The purpose of this Policy is to ensure that all use of Talbot Primary School and DET Information, Communications and Technology (*ICT*) systems is legal, ethical and consistent with the aims, values and objectives of Talbot Primary School.
- Talbot Primary School and DET ICT systems must be properly and efficiently used.
- Talbot Primary School and DET ICT systems are not to be used for inappropriate activities for example, pornography, fraud, defamation, breach of copyright, unlawful discrimination or vilification, sexual harassment, stalking, illegal activity and privacy violations.

Scope

- “Talbot Primary School and DET ICT systems” includes but is not limited to, Talbot and DET Local Area Networks (LANs), Wide Area Networks (WANs), Wireless Local Area Networks (WLANs), Intranet, Extranet, Internet, electronic mail (*Email*), computer systems, software, servers, desktop computers, notebook computers, leased notebook computers, mobile phones, digital cameras, hand held devices (for example, personal digital assistants or “PDAs”), USB memory sticks and other ICT storage devices;
- “electronic communications” means Email, instant messaging and any other material sent electronically;
- “Guidelines for Classification of Films and Computer Games 2005” means the *Guidelines for Classification of Films and Computer Games 2005* made in accordance with sub-section 12(3) of the *Classification (Publications, Films and Computer Games) Act 1995* (Cth) and effective from 26 May 2005.
- “personal use” means all non-work related use, and includes Internet usage and private Emails.
- “users” of Talbot Primary School and DET ICT systems includes all employees (including ongoing, casual and temporary employees) and contractors engaged by DET, school councils, schools, regional offices and district offices. It also includes all volunteers of DET, school councils, schools, regional offices and district offices who use DET ICT systems
- This Policy applies to all users of Talbot Primary School and DET ICT systems regardless of work location.
- This Policy applies to the use of all aspects of Talbot Primary School and DET ICT systems, networks, software and hardware collectively referred to as “*DET ICT systems*”
- Use of Talbot Primary School and DET ICT systems includes transmissions to or through DET ICT systems by a user.
- This Policy governs the use of Talbot Primary School and DET ICT systems and includes but is not limited to:
 - ❖ Publishing and browsing on the Internet (including Intranet and Extranet);
 - ❖ Downloading or accessing files from the Internet or other electronic sources;
 - ❖ Email;
 - ❖ Electronic bulletins/notice boards;

- ❖ Electronic discussion/news groups;
 - ❖ Weblogs ('blogs');
 - ❖ File transfer;
 - ❖ File storage;
 - ❖ File sharing;
 - ❖ Video conferencing;
 - ❖ Streaming media;
 - ❖ Instant messaging;
 - ❖ Online discussion groups and 'chat' facilities;
 - ❖ Subscriptions to list servers, mailing lists or other like services;
 - ❖ Copying, saving or distributing files;
 - ❖ Viewing material electronically; and
 - ❖ Printing material.
- Any reference in this Policy to an Act, Regulation, Guidelines, Code of Conduct or other document includes a reference to the Act

Rationale

- The use of Talbot Primary School and DET ICT systems carries with it responsibilities.
- The provision of Talbot Primary School and DET ICT systems by DET is to improve and enhance learning and teaching, and conduct of the business and functions of Talbot Primary School and DET. Using information technology, access in 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.
- The process by which Talbot Primary School and DET seeks to manage staff use of DET ICT systems is through the development and implementation of this Policy. The Policy must be followed whenever using DET ICT systems.

Responsibility

- 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 may include, but is not limited to -
 - ❖ providing access to a copy of the Policy;
 - ❖ reminders of the need for compliance with the Policy; and
 - ❖ providing updates or developments of the Policy, to those affected by the Policy.
- It is the responsibility of all users to abide by the Policy.

Non-Compliance

- Depending on the nature of the inappropriate use of DET ICT systems, non-compliance with this Policy may constitute:
 - ❖ a breach of employment obligations;
 - ❖ serious misconduct;
 - ❖ sexual harassment;
 - ❖ unlawful discrimination;
 - ❖ a criminal offence;
 - ❖ a threat to the security of DET ICT systems;
 - ❖ an infringement of the privacy of staff and other persons; or
 - ❖ exposure to legal liability.
- Non-compliance with this Policy will be regarded as a serious matter and appropriate action, including termination of employment, may be taken where there is a reasonable belief that illegal activity may have occurred DET will report the suspected illegal activity to the police.

Business Purposes

- The DET ICT systems are tools to be used for DET purposes.
- Use of DET ICT systems must –

- ❖ be for DET purposes only, or where authorised or required by law, or with the express permission of an Authorised Person; and
- ❖ be used like other business communications and comply with any codes of conduct, ministerial orders or legislative requirements which apply to the user, for example, the Code of Conduct for the Victorian Public Sector, the *Education and Training Reform Act 2006* (Vic) and the *Public Administration Act 2004* (Vic).
- Notwithstanding clause 6.2(a), users of DET ICT systems may use DET ICT systems for personal use provided the use is not excessive and does not breach this Policy. Users must not engage in excessive personal use of DET ICT systems during working hours. Users must not engage in excessive personal use of electronic communications and the Internet using DET networks outside working hours. A breach of either of these constitutes a failure to abide by this Policy.
- Subject to limited personal use
 - ❖ subscribing to list servers (LISTSERVS), mailing lists and other like services must be for DET purposes or professional development reasons only; and
 - ❖ on-line conferences, discussion groups or other like services must be relevant and used for DET purposes or professional development activities. Such interaction requires that internet etiquette should be observed along with current societal standards for respect and fairness.
- Obtaining unauthorised access to electronic files of others, or to Email or other electronic communications of others, is not permitted and may constitute a criminal offence under the *Crimes Act 1958* (Vic) or other legislation.
- Large downloads or transmissions should be minimised to ensure the performance of DET ICT systems for other users is not adversely affected. Where a user has caused DET to incur costs for excessive downloading of non-work related material in breach of this **DET Acceptable Use Policy – Effective from 11 July 2006** 5 policy, DET may seek reimbursement or compensation from the user for all or part of these costs.

Department Property

- DET is the owner of, and asserts copyright over, all electronic communications created by employees as part of their employment and sent through DET ICT systems.
- Electronic communications created, sent or received by the users referred to in clause 1.2 are the property of DET, 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. All information produced on computer, including emails, may be accessible under the *Freedom of Information Act 1982* (Vic). Please note that Email messages may be retrieved from back-up systems and organisations, their employees and the authors of electronic communications have been held liable for messages that have been sent.

Monitoring

- Use of DET ICT systems may be monitored by Authorised Persons.
- From time to time, Authorised Persons may examine or monitor the records of DET ICT systems including for operational, maintenance, compliance, auditing, security or investigative purposes. For example, electronic communications and websites visited may be monitored. DET may investigate a complaint arising from the use of DET ICT systems.
- Use of DET ICT systems is provided to users on condition that it is agreed that DET ICT systems are monitored in accordance with this Policy. Use of DET ICT systems constitutes consent to monitoring in accordance with this Policy.
- If at any time there is a reasonable belief that DET ICT systems are being used in breach of this Policy, the principal or line manager of the person who is suspected of using DET ICT systems inappropriately may suspend a person's use of DET ICT systems and may require that the equipment being used by the person be secured by the principal or general manager while the suspected breach is being investigated.

Defamation

- DET ICT systems 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 DET liability. Electronic communications may be easily copied, forwarded, saved, intercepted or archived. The audience of an electronic message may be unexpected and widespread.

Copyright Infringement

- The copyright material of third parties (for example, software, database files, documentation, cartoons, articles, graphic files, music files, video files, text and down loaded information) must not be used without specific authorisation to do so. The ability to forward and distribute electronic messages and attachments and to share files greatly increases the risk of copyright infringement. Copying material to a hard disk or removable disk, printing or distributing or sharing copyright material by electronic means, may give rise to personal and/or DET liability, despite the belief that the use of such material was permitted.
- DET supports the rights of copyright owners and does not and will not tolerate reckless or deliberate copyright infringement.
- All users of DET ICT systems should ensure they are familiar with the following publications issued by DET:
 - ❖ *Guidelines on Copyright and Trademark Management*; and
 - ❖ *Copyright for Schools*.

Illegal material

- DET ICT systems must not be used in any manner contrary to law or likely to contravene the law. Any suspected offender will be referred to the police or other relevant authority and their employment may be terminated.
- Illegal or unlawful use includes but is not limited to use of certain types of pornography (eg child pornography) under the *Crimes Act 1958 (Vic)*, offences under the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995 (Vic)*, defamatory material, material that could constitute racial or religious vilification, unlawfully discriminatory material, stalking under the *Crimes Act 1958 (Vic)*, use which breaches copyright laws, fraudulent activity, computer crimes and other computer offences under the *Cyber Crime Act 2001 (Cth)* or *Crimes Act 1958 (Vic)* (as amended by the *Crimes (Property Damage and Computer Offences) Act 2003 (Vic)*) or any other relevant legislation.
- In particular, DET is an institution charged with the safety and education of children. Child pornography is abhorrent and represents the antithesis of DET's responsibilities to children. Any suspected offender will be referred to the police and their employment will be terminated if the allegations are substantiated.

7

Offensive or Inappropriate material

- Use of DET ICT systems must be appropriate to a workplace environment. This includes but is not limited to the content of all electronic communications, whether sent internally or externally.
- The DET ICT systems must not be used for material that is pornographic, harassing, hateful, racist, sexist, abusive, obscene, discriminatory, offensive or threatening. This includes sexually oriented messages or images and messages that could constitute sexual harassment.
- All users of DET ICT systems should be familiar with DET anti-discrimination, equal opportunity policies and harassment policies.
- Users of DET ICT systems who receive unsolicited offensive or inappropriate material electronically should notify their manager. Offensive or inappropriate material received from people known to the receiver should be deleted and the sender of the material should be asked to refrain from sending such material again. Such material must not be forwarded internally or externally or saved onto DET ICT systems except where the material is required for the purposes of investigating a breach of this policy.

Confidentiality

- Electronic communication is not a secure means of communication. While every attempt is made to ensure the security of DET ICT systems, 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.

Viruses

- Electronic communications are potential delivery systems for computer viruses. All data, programs and files which are downloaded electronically or attached to messages should be scanned by an antivirus program before being launched, opened or accessed.
- Viruses have the potential to seriously damage DET ICT systems. Do not open any downloaded files, 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.

Attribution

- There is always a risk of false attribution of breaches of this Policy. 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. 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.
- Users are accountable for all use of DET ICT systems that have been made available to them or leased to them for work purposes and all use of DET ICT systems performed with their user-ID. Users must maintain full supervision and physical control of DET ICT equipment, including notebook computers, at all times. User-IDs and passwords must be kept secure and confidential. User-IDs and passwords should not be disclosed to anyone, including disclosure to line managers or above. Users must not allow or facilitate unauthorised access to DET ICT systems through the disclosure or sharing of passwords or other information designed for security purposes.
- Active connections are to be terminated when access is no longer required and PCs secured by password when not in use.

Mass distribution and 'Spam'

- The use of electronic communications for sending 'junk mail', forprofit messages, or chain letters is strictly prohibited.
- Mass electronic communications should only be sent in accordance with normal DET procedures.
- The use of electronic communications for sending unsolicited commercial electronic messages ('Spam') is strictly prohibited and may constitute a breach of the *Spam Act 2003* (Cth).

Records Management

- Electronic Communications are public records and subject to the provisions of the *Public Records Act 1973* (Vic).
- DET record management practices for management of Email messages must comply with DET policies and guidelines on recordkeeping and management of electronic communications as amended from time to time.
- 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.
- 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 mail box. Messages for archive should be kept in separate archive files stored on the user's network home or shared drive.

Disclaimer

- All emails sent externally from DET's Edumail service will automatically have a disclaimer attached to them. The current disclaimer is worded as follows: "*IMPORTANT - This email and any attachments may be confidential. If received in error, please contact us and delete all copies. Before opening or using attachments, check them for viruses and defects. Regardless of any loss, damage or consequence, whether caused by the negligence of the sender or not, resulting directly or indirectly from the use of any attached files our liability is limited to resupplying any affected attachments. Any representations or opinions expressed in this email are those of the individual sender, and not necessarily those of the Department of Education & Early Childhood Development.*"
- This disclaimer must not be altered or interfered with in any way, except by Authorised Persons. The use of this disclaimer may not necessarily prevent DET or the sender of the email from being held liable for its contents.
- School eMail systems must also append the same disclaimer (above) to messages sent externally from the School's Email service.

Complaints

- If you wish to make a complaint about an electronic communication which is offensive or inappropriate, raise it with your line manager or, if your line manager is the cause of your complaint, raise it with your line manager's manager.

Breaches of this Policy

- Breaches of this Policy may be categorised using the following categories. The categories do not cover all breaches of this Policy, for example the categories do not specifically refer to breaches of copyright. Matters not covered by the following categories will be dealt with on an individual basis and on the relevant facts.

Category 1: Illegal

This category covers the following:

- ❖ **Child pornography** – offences relating to child pornography are covered by the *Crimes Act 1958* (Vic) and the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Child pornography is defined in section 67A of the *Crimes Act 1958* (Vic) as: "a film, photograph, publication or computer game that describes or depicts a person who is, or appears to be, a minor engaging in sexual activity or depicted in an indecent sexual manner or context."
- ❖ **Objectionable material** – offences relating to the exhibition, sale and other illegal acts relating to "objectionable films" and "objectionable publications" are covered by the *Classification (Publications, Films and Computer Games) (Enforcement) Act 1995* (Vic). Such material has or would attract a classification of **X18+ (restricted)** or **RC (refused classification)** under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth).
- ❖ Any other material or activity which involves or is in furtherance of a breach of the criminal law.

Category 2: Extreme

- This category involves non-criminal use of material that has or would attract a classification of **RC** under the Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). This covers any material that:
 - ❖ depicts, expresses or otherwise deals with matters of sex, drug misuse or addiction, crime, cruelty, violence or revolting or abhorrent phenomena in such a way that they offend against

the standards of morality, decency and propriety generally accepted by reasonable adults to the extent that the material should not be classified;

- ❖ describes or depicts in a way that is likely to cause offence to a reasonable adult, a person who is, or **DET Acceptable** appears to be, a child under 18 (whether or not the person is engaged in sexual activity or not); or
- ❖ promotes, incites or instructs in matters of crime or violence

Category 3: Critical

- This category involves other types of offensive material. This covers any material that:
 - ❖ Has or would attract a classification of **X18+** under Guidelines for Classification of Films and Computer Games 2005 or National Classification Code scheduled to the *Classification (Publications, Films and Computer Games) Act 1995* (Cth). The material covered by this classification is only available for hire or sale in the ACT and Northern Territory, and covers sexually explicit material that contains real depictions of actual sexual intercourse and other sexual activity between consenting adults;
 - ❖ Involves racial or religious vilification;
 - ❖ Is unlawfully discriminatory;
 - ❖ Is defamatory;
 - ❖ Involves sexual harassment; or
 - ❖ Brings or has the potential to bring the employee and/or DET into disrepute.

Category 4: Excessive personal use during working hours

- This category covers personal use which satisfies the following 3 criteria -
 - ❖ . it occurs during normal working hours (but excluding the employee's lunch or other official breaks); and
 - ❖ it adversely affects, or could reasonably be expected to adversely affect the performance of the employee's duties; and
 - ❖ the use is more than insignificant.

The agreement below is to be signed by the student and parent.

When I use technology, both at school and at home I have responsibilities and rules to follow. I agree to:

- be a safe user whenever and wherever I use that technology.
- be responsible whenever and wherever I use technology and support others by being respectful in how I talk to and work with them and never write or participate in online bullying. This includes forwarding messages and supporting others in harmful, inappropriate or hurtful online behaviour.
- report to an adult if I feel unsafe or uncomfortable online or see a friend being unsafe or being made to feel uncomfortable by others.

When at school I agree to:

- behave in a way outlined in the schools' Code of Conduct when online or using mobile technology.
- keep myself and my friends safe by not giving out personal details including full names, telephone numbers, addresses and images and protecting my password
- use the technology at school for learning, use the equipment properly and not interfere with the work or data of another student
- not bring or download unauthorised programs or files
- not go looking for rude or offensive sites
- use an 'online name' and avatar when sharing my work online.

- remember that the content on the web is someone’s property and ask my teacher / parent to help me get permission if I want to use information or pictures
- think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information as my answer).
- talk to my teacher or another adult if:
 - I need help online
 - I am not sure what I should be doing on the internet
 - I come across sites which are not suitable
 - someone writes something I don’t like, or makes me and my friends feel uncomfortable or asks me to provide information that I know is private
 - I feel that the welfare of other students at the school are being threatened

If requested by a teacher to bring a mobile phone, iPod or other mobile device at school I agree to:

- use it as requested for learning purposes as directed by my teacher
- be responsible in my use and not use the device to find, create or send information that might be harmful, inappropriate or hurtful to me or anyone else.

When using my mobile device as a camera I will:

- only take photos and record sound or video when it is part of a class or lesson
- seek permission from individuals involved PRIOR to taking photos, recording sound or videoing them (including teachers)
- seek written permission from individuals involved PRIOR to publishing or sending photos, recorded sound or video to anyone else or to any online space
- be respectful in how I talk to and work with others online and never write or participate in online bullying
- seek teacher permission before uploading any content to websites, blog etc

This Acceptable Use Policy for Mobile Devices also applies to students during school excursions, camps and extra-curricula activities.

I acknowledge and agree to follow these rules. I understand that my access to the Internet and mobile technology at school will be renegotiated if I do not act responsibly.

Student Name:.....

Student Signature:.....

Parent Permission

I agree to allow my child to use the Internet at school. I have discussed the scenarios, potential problems and responsible use of the Internet with him/her as outlined in the Internet use kit. I will contact the school if there is anything here that I do not understand. If there is a situation which concerns me, I will contact either the school or ACMA Australia's Internet safety advisory body on 1800 880 176.

Parent/Guardian Signature :

Date:.....

Talbot Primary School uses the Internet as a teaching and learning tool. We see the Internet and mobile technology as valuable resources but acknowledge they must be used responsibly.

Your child has been asked to agree to use the Internet and Mobile technology responsibly at school. Parents should be aware that the nature of the Internet means that full protection from inappropriate content can never be guaranteed.

At **Talbot Primary** we:

Have a cyber safe and responsible use program across the school. We reinforce the school code of conduct values and behaviours when using technology and the internet.

- provide a filtered Internet service
- provide supervision and direction in Internet activities and when using mobile technologies for learning
- utilise mobile technologies for educational purpose. e.g. Podcasts, photos from excursions
- work towards setting tasks that ask your child open questions, so they can't copy and paste all answers from the Internet
- provide support to parents to understand this agreement
- provide support to parents through an information evening and as a document attached to this agreement.

Evaluation:

- This policy will be reviewed as part of the school's three year review cycle.

This policy was last ratified by School Council in....

2015

Principal's signature: _____

School Council President's signature: _____

Date: _____

Advice for Parents

Please keep this as a resource to use at home

At school the Internet is mostly used to support teaching and learning. At home, however, it is often used differently. Not only is it a study resource for students, but it is increasingly being used as a social space to meet, play and chat. The Internet can be lots of fun.

If you have the Internet at home, encourage your child to show you what they are doing online. If not, see if you can make a time to visit the school to see their work and how the school uses the Internet.

Bullying, stranger danger, gossip, telling the wrong people personal information about yourself have long been issues for young people growing up. These are all behaviours which now present online. These are not “Virtual” Issues. They are real and can harm and hurt.

At home we recommend you:

- make some time to sit with your child to find out how they are using the Internet and who else is involved in any online activities
- ask them to give you a tour of their “space” if they are using a site which allows them to chat, publish photos, play games etc
- always get them to set the space to “Private” if they use a social networking site like Myspace, Bebo, Pixa etc – They are then in control of who contacts them and can access their information. They can block out anyone at anytime.
- have the computer with Internet access in a shared place in the house – not your child’s bedroom
- negotiate appropriate times for your child’s online activities and use of mobile phones.
- ask questions when your child shows you what they are doing
 - how does it work and how do you set it up? Can you block out people?
 - who else is sharing this space or game - did you know them before or “meet” them online? What do you know about them?
 - why is this so enjoyable – what makes it fun?
 - can you see any risks or dangers in the activity - what would you say to warn/inform a younger child who was going to start to use the space?
 - what are you doing to protect yourself or your friends from these potential dangers?
 - when would you inform an adult about an incident that has happened online that concerns you? Discuss why your child might keep it to themselves.

Many students say they will not tell an adult they are in trouble or ask for help because:

- they might get the blame for any incident
- they don’t think adults “get” their online stuff – it is for students only
- they might put at risk their own access to technology by either:
 - admitting to a mistake or
 - highlighting a situation that might lead a parent to ban their access. (Even to protect them)