1.1. Policy title: COMMUNITIES ONLINE: ACCEPTABLE USE OF ICT – PARENTS AND STUDENTS

Published: 2013

Identifier: TBA

Legislation:

- ***Copyright Act 1968***
- ***Copyright Amendment (Digital Agenda) Act 2000***
- ***Copyright Amendment (Moral Rights) Act 2000***
- ***ACT Education Act 2004***
- ***Education (Participation) Amendment Act 2009***

Procedures:

- Acceptable Use of ICT Guidelines
- Use of Third Party Web-based Educational Services Guidelines and Mandatory Procedures

2. POLICY STATEMENT

2.1. The Education and Training Directorate (the Directorate) is committed to the use of Information and Communication Technology (ICT) in ACT public schools.

2.2. Students will use ICT in a variety of ways including class work, homework, projects and assignments; as well as collaboration and communication with others (including - but not limited to – students, teachers, guest speakers, community members and international experts) across the ACT and around the world - sharing ideas, challenges, knowledge and information.

2.3. Effective use of ICT allows schools to strengthen communication with parents and carers, and streamline administrative processes.

2.4. Usage of ICT resources, including online services and personal electronic devices, both on and off school grounds is provisional on the expectation that it be consistent with the terms and conditions of this policy, the school's code of conduct and student welfare policy.

2.5. Prior to accessing the resources provided by the Directorate, students and parents are required to read this policy (as well as any attached documents) and, where applicable sign an Acceptable Usage Statement.

2.6. The Directorate, and the school as its representative, reserves the right to revoke, suspend or terminate the access permissions of any user at any time, with or without notice.

2.7. Users should be aware that usage data will be logged, maintained, backed-up, archived and monitored for computing activities accessing ACT Government networks and resources. This includes workstations, laptops, servers, printers, network connected devices, and personal electronic devices including (but not limited to) smart phones and tablets.

2.8. Whilst the Directorate provides filtering that will minimise inadvertent access to inappropriate content on the internet, it is not possible to guarantee that students will not be exposed to inappropriate content at school. Students who seek to deliberately circumvent these filters will be considered to be in breach of this policy and will be sanctioned accordingly.

3. RATIONALE

3.1. This policy and its attached guidelines defines the parameters of acceptable usage by students and parents of ICT resources provided by, and through, the Directorate.

3.2. This policy applies to all those enrolled to attend a school, course or program administered by the Directorate and those members of the school community, such as parents and carers, who access Directorate ICT services and resources.

3.3. Those employed by the ACT Government, including those on Australian School-Based Apprenticeships and Work-Experience placements, are classified as *'workers'* under the Whole-of-Government Acceptable Use of ICT Resources Policy *(policy no. WhoG-136)* managed by Shared Services – ICT. As such, their acceptable usage of ICT resources is to be managed under the auspices of that policy.

4. DEFINITIONS

5.

5.1. The Directorate refers to the ACT Education and Training Directorate.

5.2. **ICT resources** refers to the hardware, software, and services related to information and communication technologies (ICT).

5.3. A **parent** is a person with legal parental responsibility for the student. This includes carers and legal guardians.

5.4. **PEDs or Personal Electronic Devices** refers to (but is not limited to) workstations, laptops, tablet devices and smart phones which are owned by individual users and brought to the school.

5.5. **Schools** refer to ACT public schools.

5.6. **Student(s)** includes all those enrolled in years P-12 to attend an ACT public school, course or program administered by the Directorate.

5.7. **Third Party Web Services** refers to external web services used in an educational capacity that are not hosted within the Directorate's environment.

5.8. **Users** refers to students, parents, guardians and community members that access the Directorate's ICT resources.

6. LEGISLATION

6.1. The *Education Act 2004 (ACT)* allows for the exclusion of students from school activities if their actions compromise the good name of the school or the safety or wellbeing of other students. This includes online activities.

6.2. The *Copyright Act 1968 (Cwlth)* defines the acceptable use of copyright material.

7. PROCEDURES

7.1. Prior to accessing the Directorate's ICT resources, students and parents are required to read this policy and the attachment *Acceptable Use of ICT Guidelines* and then sign an Acceptable Usage Statement. Examples are available in Attachment A – Acceptable Use Statement

7.2. The *Use of Third Party Web-based Education Services Guidelines and Mandatory Procedures* document outlines the responsibilities of schools, students and parents when accessing third party websites for educational use.

8. POLICY OWNER

9.

9.1. Director: Information, Communications and Governance. For support in relation to this policy, please contact the Directorate's Chief Information Officer on (02) 6205 6749.

10. RELATED POLICIES

10.1. **ACT Education and Training Directorate Review of Decisions policy**
10.2. ACT Education and Training Directorate Complaints Resolution policy
10.3. ACT Education and Training Directorate Critical/Non-Critical Incident Management and Reporting policy
10.4. ACT Education and Training Directorate Providing Safe Schools policy
10.5. ACT Education and Training Directorate Countering Bullying, Harassment and Violence in ACT Public Schools policy
10.6. ACT Education and Training Directorate Countering Racism in ACT Public Schools policy
10.7. ACT Education and Training Directorate Countering Sexual Harassment in ACT Public Schools policy
10.8. Shared Services ICT (policy no. WhoG-136) Acceptable Use of ICT Resources policy
10.9. Shared Services ICT (policy no. WhoG-116) ICT Security policy
10.10. Shared Services ICT (policy no. WhoG-134) Mobile Devices policy

Acceptable Use of ICT Guidelines

Appropriate use provisions

1. Users must not create, send or access information that could damage the ACT Government's reputation, be misleading or deceptive, result in victimisation or harassment, lead to criminal penalty or civil liability, or be reasonably found to be offensive, obscene, threatening, abusive or defamatory. This includes pornography and other offensive material. Material may be pornographic under the *Criminal Code 1995 (Cth)* even if it features fictional or cartoon characters. The transmission, storage or downloading of obscene or offensive material may also put users at risk of breaching discrimination laws.

2. In addition to prohibited material, there are categories of internet content that are considered inappropriate for access through ACT Government ICT resources. To address this, Shared Services ICT has deployed a content filter to monitor Internet access. This filter intercepts web requests and determines whether the site being accessed is acceptable under the terms of this policy. If the filter determines that a site falls outside the policy, the site will either be blocked or a warning screen will be displayed advising that the site appears to be in breach of the policy. The content filter will warn or block access to categories of websites including:

    a. adult content
    b. gambling
    c. unsupervised chat rooms
    d. dating
    e. crime/terrorism
    f. violence/undesirable activities
    g. malicious
    h. government blocking list (illegal websites)
    i. swimsuit/lingerie models.

3. Should users need to access legitimate sites for their work but find them filtered, they will need to seek permission from their school's ICT Coordinator or relevant executive teacher, under delegation from the school Principal, to arrange for approved access to the sites.

4. Users must not create, send, access, download or store inappropriate or prohibited material.

5. Users must not use Government resources to encourage others to engage in industrial action.

Logging and Monitoring

The following information about logging and monitoring of the network is taken from the *ACT Government's Whole of Government Acceptable Use Statement.* While it refers specifically to staff, the same principals and processes apply for students and their families when they are accessing the ACT Government's ICT resources.

Logging refers to the automated collection of transaction records. Monitoring includes active, ongoing surveillance by Shared Services ICT Security under the Senior Manager, Shared Services ICT Security. This document describes the way in which employees' activities may be monitored and how employees should be notified that this monitoring is being carried out.

ACT Government monitors staff use of Government computers and ICT systems by:maintaining logs, backups and archives of computing activities including workstations, laptop computers, servers, printers, and network connected devices, including smart phones and tablets (where applicable); monitoring email server performance and retention of logs, backups and archives of emails sent and received through ACT Government servers; and retaining logs, backups and archives of all Internet access and network usage.

Shared Services ICT Security has access rights to logs of all of staff members' activity including: backups and archives of all files, including emails, which are current and those that have been deleted by the user, email messages and attachments and the URLs or website addresses of sites visited, the date and time they were visited and the duration of site visits and logs.

Shared Services ICT Security in consultation with the Directorate Executive may authorise access to user logs in the event that there is a perceived threat to:

- ACT Government ICT system security,
- the privacy of ACT Government staff,
- the privacy of others, or
- the legal liability of the ACT Government.

These records can be called up and cited as a chain of evidence in legal proceedings and actions following virus attacks. Access will be fully logged and documented.

Shared Services ICT will not disclose the contents of monitoring to a person, body or Directorate (other than the individual concerned) unless one or more of the following applies:

- the staff member is reasonably likely to have been aware, or made aware that information of that kind is usually passed to that person, body or Directorate;
- they have consented to the disclosure;
- Shared Services ICT believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
- the relevant Directorate Executive has requested monitoring or investigation;
- the disclosure is required or authorised by or under law;
- the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.
- Shared Services ICT may log on a random or continuous basis:
- for system management and planning,
- to ensure compliance with ACT Government policies,
- to investigate conduct that may be illegal or adversely affect ACT Government employees, or
- to investigate inappropriate or excessive personal use of ACT Government ICT resources.

Under the provisions of the Workplace Privacy Act, employers must – upon being requested by the worker – provide access to the worker's surveillance records. Workplace surveillance records will be kept in accordance with the requirements of the Territory Records Act.

Reporting misuse, breaches and inappropriate material

Schools MUST report any suspected illegal activity, security incidents and other incidents of a serious nature in accordance with the ACTETD *Critical/Non-Critical Incident Management and Reporting* policy and procedures.

Schools must report to the Shared Services ICT Service Desk without delay any suspected technical security breach by users. Shared Services ICT are then responsible for following up on these complaints.

Low-level breaches of acceptable usage provisions may be managed at the school level in accordance with the Directorate's Review of Decisions and Complaints Resolution policies.

Where disputes arise in the handling of such breaches and cannot be resolved at the school level, they are to be escalated in line with the Directorate's *Review of Decisions and Complaints Resolution* policies.

Access and security

Prior to accessing the Directorate's ICT resources, students and/or parents and guardians are required to read these guidelines and the accompanying policy: Communities Online (Acceptable Use of ICT – Parents and Students). All parents/guardians (with the exception of those whose children have already turned 18) are required to sign an Acceptable Use Statement. Schools may also ask students to sign an Acceptable Use Statement, depending on their age and level of understanding. Examples of forms that may be used by schools are in Appendix i.

Schools must inform parents of their right to have their child *'opt out'* of using all or part of the online services available through their school.

Schools are responsible for ensuring that their school communities have regular access to information relating to cyber-safety. Schools are also responsible for provisioning usage monitoring and internet filtering in the delivery of ICT resources

School responsibilities

It is the duty of each school to ensure that their school community is aware of their responsibilities under this policy.

Schools must:

- Inform their school community of this policy's existence.
- Make this policy (and its associated guidelines) available to parents/guardians and members of the school community.
- Ensure that school communities are adequately informed about the use of the ICT resources within their school community.
- Ensure that school communities are informed of their rights and responsibilities relating to ethical and safe usage of ICT resources.
- Provide students equitable access to online services-enabled computers within the limits of available resources.

Personal Electronic Devices

The network is configured to enable filtered internet access through Personal Electronic Devices (PEDs). The decision to promote the use of PEDs within a school is at the discretion of each school Principal.

While the Directorate will make every reasonable effort to provide a safe, secure and appropriate online learning experience for school communities, the Directorate cannot filter, monitor and control private telephone mobile access on PEDs that are using 3G/4G type networks. However, existing student welfare and behaviour management practices already in the school would apply to their use. Similarly, the individualised nature of PEDs means that the Directorate is unable to provide technical support.

Usage of PEDs on school grounds, whether accessing the Directorate network or not, is provisional on the expectation that it complies with the terms and conditions of this policy.

Appendices

i. Sample Acceptable Use of ICT Statement – Parents/Guardians: An example of an Acceptable Use statement that schools could provide for students and parents to sign. This may be adapted to suit the needs of the school and the age level/ability of the student.
ii. Sample Acceptable Use of ICT Statements – Students: While it is important that parents acknowledge the policy in relation to their child, some schools might also have their students sign an Acceptable Use statement. Included in Appendix ii are some examples that may be used or modified to suit individual school contexts.

Appendix i – Sample Acceptable Use Statement : Parents or Guardians

Acceptable Use of ICT Statement – Parents /or Guardians

ACT Education and Training Directorate (ACTETD) public schools operate within various policy guidelines that support the rights and expectations of every member of the school community to engage in and promote a safe and inclusive educational environment. This environment includes (but is not limited to) the ACTETD's computer network; Personal Electronic Devices (PEDs) that connect to its networks; online applications hosted within the ACTETD's secure environment (e.g. Digital Backpack, Oliver) as well as online and/or cloud environments outside of the ACTETD's secure online environment.

According to the Melbourne Declaration on the Educational Goals for Young Australians (MCEECDYA, 2008)[1]: "in a digital age, and with rapid and continuing changes in the ways that people share, use, develop and communicate with ICT, young people need to be highly skilled in its use." The ACTETD recognises the need for students to engage with ICT resources and that the safe and responsible use of these technologies – including online behaviour – is best taught in partnership with parents and/or guardians.

To ensure the security of the network and users, the ACTETD may authorise access to user logs in the event that there is a potential breach of the conditions of this policy, which may pose a threat to:

- System security
- Privacy of staff and students
- Privacy of others
- Legal liability of the ACT Government
- Student welfare

By signing this statement, you acknowledge the procedures and guidelines outlined in the Communities Online: Acceptable Use of ICT– Parents and Students Policy and agree to your child accessing ICT resources in ACT schools.

1 http://www.mceecdya.edu.au/verve/_resources/national_declaration_on_the_educational_goals_for_young_australians.pdf

---

Acceptable Use of ICT Statement - Parent and/or Guardian Consent

I have read and understand the *Communities Online: Acceptable Use of ICT– Parents and Students Policy* and its associated procedural documents: *Acceptable Use of ICT Guidelines* and *Use of Third Party Web Based Educational Services Guidelines*. I understand the need for my child to be a safe and responsible user of ICT resources – including the use of PEDs, and support the ACTETD in the implementation of the policy guidelines as outlined in the *Communities Online: Acceptable Use of ICT Resources* Policy. I have discussed this information with my child.

I agree to my child having access to (please circle):

School computers, local applications, and network drives Yes No

Note: if you select No, this will automatically prevent your child from accessing any of the other services below.

* Internet Yes No
* Internal (school) email Yes No
* cLc and/or MyLearning Yes No

Name of child (printed):

Parent and/or Guardian (Name printed):

Parent Signature: Date:

Appendix ii – Sample Acceptable Use Statements – Students

Acceptable Use of ICT Statement – Students

The Acceptable Use of ICT statement for parents and guardians should be signed by all parents/guardians of students under the age of 18. Students aged 18 and above can sign the form themselves.
In addition to this, schools may wish to have their students sign an additional Acceptable Use Statement. This ensures that students are aware of their responsibilities when using ICT resources, as well as the consequences of any breach.

The ACTETD caters for students aged between 3 and 19. As such, it is difficult to create a generic statement that will suit the needs and understanding of each of these students.
The examples on the following pages were sourced from ACT schools and may be used as the basis for developing an acceptable use statement that is relevant to the students in specific school contexts.

In any acceptable use statement to be used by students, it is important to include the following:

- A summary of acceptable/non-acceptable behaviour
- Consequences for the breach of the acceptable use conditions
- A statement that the student agrees to when signing the form

When students sign an Acceptable Use of ICT Statement, they are agreeing to the conditions of this policy and agree to accept the consequences of any breach. While this policy deals specifically with the use of ICT resources, it is important to remember that school-based behaviour management policies and procedures apply to online behaviour, just as they do to physical behaviour in the school. Just as bullying, harassment or abuse would not be tolerated in the classroom or on the playground; they are similarly not tolerated within online environments. Any online breaches of the school's behaviour policies should be dealt with as they would had they occurred in the physical environment.

Appendix ii – Sample Acceptable Use Statements – Students

Primary School Acceptable Use of ICT Code of Practice for Students – example 1

When using ICT resources at Primary School (including the student network, internet, email, Digital Backpack, laptops, IWBs etc):

- I will use school computers only with the permission of a teacher.
- I will follow all instructions from teachers when using school computers.
- I will not let anyone else know my passwords or usernames.
- I know that I am responsible for anything that happens when my account is used.
- I know that the school and the Education and Training Directorate receives information about anything that I send or receive.
- I will tell my teacher if I think someone has gained access to my account
- I will make sure any email I send or any work that I wish to have published is polite and carefully written and presented.
- I will respect other students' work and ensure appropriate feedback about individual responses.
- I will not read other people's emails.
- I will not tell anyone my address or telephone number or the address or telephone number of anyone else or send photographs of myself or others.
- I will use material from other websites only if I have permission to do so.
- If I use material in my work that I have found on the internet, I will say where it comes from.
- If I see or receive any information on the computer that makes me feel uncomfortable or is inappropriate I will tell a teacher straight away, or report it using the Cyber Safety Button on the Digital Backpack.
- I will not damage or disable the computers, computer systems or computer networks of the school.

I have read and understand the Primary School Acceptable Use of ICT Code of Practice for Students. I understand that disciplinary action may be taken if I do not follow this agreement, which may include loss of access to the internet, cLc, or school network or the use of ICT for a period of time.

Student:
I agree to follow the Code of Practice and any other relevant rules that are set by Primary School:

Name: **Class**:

Signed: **Date**

Once this form is signed by student and parent/carer please return to class teacher.

Appendix ii – Sample Acceptable Use Statements – Students

Primary/Middle School - Acceptable Use of ICT Code of Practice for Students – example 2

This code of practice was developed for students of Primary School and is consistent with the Directorate's Communities Online Policy. All students will need to read and sign this document before utilising the school ICT equipment.

- I will use the school computers for school work only and only as directed by my teacher.
- I will be courteous and use appropriate language when communicating to others.
- I will ask my teacher for help if I find or receive information that I feel uncomfortable with or is inappropriate.
- I will not use the school computer facilities for illegal or dishonest purposes.
- I will not copy software programs on school computers, or copy material, graphics or music owned by others without their permission.
- I will not send, produce, show or search for things that might upset others.
- I will not intentionally create network congestion or disrupt the school computer equipment.
- I will not tell other people my password or leave the computer logged in when leaving the room.
- I will not send photographs or publish full names or personal details of others or myself to unknown people without permission.
- I will not send email to users outside of this school unless the teacher approves it.
- I understand that the school records where I have gone on the Internet

I understand that not following this Code of Practice may lead to loss of internet, email or networks access for a period of time determined by the Principal.

Student Declaration

Students of School may access the Internet and Email after signing the following declaration.
I declare that I have read and/ or understand the Student Code of Practice for School.

Student's Name:

Year/Class:

Signature :

Date:

High School/College- Acceptable Use of ICT Code of Practice for Students – example 3

The (school) has a number of facilities which enable you to access information on computer networks such as the Internet.

To ensure fair and equitable access for all members of the college community who wish to make use of these facilities, all users are required to sign an agreement to abide by certain rules which are described in a code of practice. Most of these rules are ones you would be expected to follow on any computer network.

To make use of the college's networked computing facilities, please ensure that you have read and understood the following code of practice, then sign the agreement below.

Code of Practice

When using the College's facilities to access computer networks:

YOU MAY

- find, copy, and/or print information required for any of your college courses;
- collaborate or share information relevant to your courses with students or teachers in other schools;
- download files containing information or software relevant to any of your college courses where this action does not involve a breach of copyright laws;
- undertake any other special project which is approved by a teacher at the College
- access e-mail through a web-based account.

YOU MAY NOT

- e-mail or display offensive messages or pictures;
- use obscene language;
- harass, insult or attack others;
- damage computers, computer systems or computer networks, for example, by propagating viruses or interfering with system configurations;
- violate any laws, for example, those related to copyright and privacy
- use others' passwords;
- trespass in others' folders, files or systems;
- intentionally waste limited resources;
- use the network for commercial purposes;
- use the network for any purpose that is not directly related to your studies at (school).

VIOLATIONS OF THESE RULES MAY RESULT IN

- loss of access;
- legal action if appropriate.

I have read and understood the (school) Students' Code of Practice.

I agree to abide by the code and any other relevant rules that may be set by the college.

Name: **ID No:**

Signed: **Date:**

Use of Third Party Web Based Educational Services Guidelines and Mandatory Procedures

These guidelines should be read in conjunction with the *Communities Online: Acceptable Use of ICT– Parents and Students Policy* 2013

The ACT Education and Training Directorate provides access to a range of online services for use in educational settings. These services are hosted on the Directorate's network and all data related to these services is contained within the ACT. These services include the Oliver library system, Adobe Connect and the Digital Backpack, but do change from time to time.
While these services are used by many students across the Directorate, they don't always meet the needs of individual classrooms or school programs. As a result, schools often use 'third party' services that exist on the external internet. These include sites like Mathletics, Edmodo, Facebook and similar websites. While each site is different, it's important to remember that these sites are not housed within the Directorate's network and as such, are not subject to the same data management policies or security measures. While the use of these sites can be an important part of a school's educational program, it is important for students, parents and guardians to understand how these sites will use personal data.

It is important that all schools understand their obligations when utilising third party web based service providers with regard to the Privacy Act 1988 (Cth). It is clearly stated within the Privacy Act that releasing information about students which may include names or the opportunity for students to self disclose their identity, without first seeking clear permission from parents and/or guardians, is in breach of the Privacy Act.

In light of this, Schools are required to be proactive and consider the curriculum to be covered during the year and determine if the services of a third party web based provider might be utilised as a component of the curriculum and the information that will be disclosed as a result of using those web based services.

Be aware that the guidelines only pertain to your school's relationship with *third party* web service providers. Web and software based services that are provisioned by the Directorate and Shared Services ICT have very strict rules around data sovereignty and student information is protected from external sources. There is no need to seek permission from parents or legal guardians for web services supplied by the Directorate, as this is covered by the signed consent: 'Acceptable Use of ICT Statement'.

Prior to approving the implementation of third party web services that utilise student data or web services that allow students to self disclose personal data, the Principal must ensure that they are familiar with the web service provider's privacy terms and conditions, particularly with regard to whom the provider may further disclose student's information.

1. **Where third party web service providers require student's personal information, the school must:**

- Notify parents/legal guardians about the service provider's requirements and its privacy terms and conditions.

- Summarise key information from the site's terms and conditions or privacy policy. Language that describes the way data is used by third party service providers should be clear and unambiguous.
- It is important that this step is completed explicitly for each separate web service utilised by the school.

2. Any third party web service recommended by the school that utilises student data or allows students to self disclose personal data can only be used by a student with signed parental/guardian approval. This approval will be accompanied by clear advice. The advice to the parent/legal guardian will include:

- The name of service provider and type of service provided (e.g. mathematics support, science extension, etc).
- Details which include a link to the service provider's website, particularly its terms and conditions.
- The reasons why the website is collecting the information, what laws authorise the collection, what the information will be used for, and advice regarding the use of that data by any other body or service.
- Printed details of the service provider website. In particular the terms and conditions information. Relevant information about that websites use of student data should be highlighted for ease of comprehension, allowing parents and guardians to make an informed decision about permitting the release of student information.

3. The school must keep a record of each approval to utilise third party web services for each student as part of their student file. The school must:

- Ensure that all records of the Directorate held by the school comply with the *Territory Records Act 2002*. Student Permission forms signed by parents are considered administration forms that should be placed on the Student's STUDENT ADMINISTRATION - Case Management File (Student File). These records are held for the life of the file in accordance with the following disposal class: Australasia - Destroy when person reaches 25 years of age, or 7 years after last action, whichever is later.

Appendices

iii. Template Permission form for Parents/ Legal Guardian – This template can form the basis for school based permission slips and contains all required fields of information.
iv. Sample permission form for Parents / Legal Guardian – This is an example of the type of permission letter that should be sent to parents when requesting permission for students to use Third Party Web Services.

Appendix iii – Template Permission Letter

Dear parent/guardian,

(School) is committed to providing a technology rich environment for our students as our community believes the use of Information and Communication Technology (ICT) is fundamental in assisting teaching and learning in all areas of the school curriculum.

The use of web based learning resources and cloud based storage has risen steadily over the last decade and are increasingly being used by teachers across the Directorate to improve student learning outcomes.

Teachers make decisions designed to assist students in their learning. Sometimes it is beneficial for the student to utilise services provided by third party web based providers. Types of services provided by these service providers include online content creation, collaborative tools, online educational games and various administrative programs for tracking student assessment data.

As our school wishes to register with a web based service provider that requires some personal information about a student in your care, I am obliged under the Commonwealth Privacy Act (1988) to advise you of the reasons for collecting the information, what will be done with it and who else may have access to it.

The below site has been identified as being a useful component in: (SUBJECT)

Name of Provider:
Type of Service:
Website:
Summary Terms and Conditions:
Terms & Conditions Link:

Please return this form once completed.

Student's name:

Parent/Guardian's Name:

I **consent / do not consent** (please circle your choice) to our child's information to be supplied

To:

For the purpose of:

Parent/Guardian's Signature:

Date:

ATTACHMENT B – Third Party Web Services Guidelines

Dear parent/guardian

Hedley Beare School is committed to providing a technology rich environment for our students as our community believes the use of ICT is a fundamental in assisting teaching and learning in all areas of the school curriculum.

The use of web based learning resources and cloud based storage has risen steadily over the last decade and are increasingly being used by teachers across the Directorate to improve student learning outcomes.

Teachers make decisions designed to assist students in their learning. Sometimes it is beneficial for the student to utilise services provided by third party web based providers. Types of services provided by these service providers include online content creation, collaborative tools, online educational games and various administrative programs for tracking student assessment data.

As our school wishes to register with a web based service provider that requires some personal information about a student in your care, I am obliged under the Commonwealth Privacy Act (1988) to advise you of the reasons for collecting the information, what will be done with it and who else may have access to it.

The below site has been identified as being a useful component in: Year 10 English. Using a shared learning space on the EdLearnSpace website will allow the Year 10 English Classes to share ideas, comment on each other's work and publish their assignments for viewing by other students and marking by their teachers. The forums in EdLearnSpace will be vital in creating a collaborative working space for Year 10 students as they complete the class work as part of the Macbeth unit. Accessing EdLearnSpace is not restricted to school and students will be able to access the website from home to answer homework questions, talk to other students and seek clarification from their teachers. We believe the EdLearnSpace site makes sufficient effort to protect the privacy of its users as outlined in their Privacy policy below. Relevant sections of that policy have been highlighted for you.

If you have any further questions about the implications of signing this permission slip or you would like to seek further clarification around the use of the website please do not hesitate to contact me.

Principal
Hedley Beare School
March 2013

Name of Provider: EdLearnSpace
Type of Service: Virtual Learning Community
Website: http://www.EdLearnSpace.com/

Summary Terms and Conditions:

EDLEARNSPACE PRIVACY POLICY

Effective date: January 4, 2013

EdLearnSpace makes the following assurances in regards to privacy and student data:

- We receive and store any information you knowingly enter on the Services, whether via computer, mobile phone, other wireless device, or that you provide to us in any other way. This information may include, without limitation, Personal Information such as your name, user name, email address, phone number, profile picture, school affiliation and location, billing and payment information (as it relates to Credit and the EdLearnSpace Store), and any other information necessary for us to provide our Services. If you are a student registrant, the only Children's Personal Information we require is your name and user name; through the functionality of the Services, you may also be permitted to input a profile picture and an email address or phone number.
- We receive and store certain types of usage information whenever you interact with the Services; this information is not Personal Information or Children's Personal Information.
- Cookies are alphanumeric identifiers that we transfer to your computer or mobile device to enable our systems to recognize your computer or device and tell us how and when pages in our site are visited and by how many people. EdLearnSpace cookies do not collect Personal Information or Children's Personal Information, and we do not combine the general information collected through cookies with other Personal Information or Children's Personal Information to tell us who you are or what your user name or email address is.
- We use the Children's Personal Information for creating your individual account (which will identify you within your Limited Access Groups), customizing your experience, and for sending you notifications via the Services from your teacher, school, district, fellow Limited Access Group members, and from EdLearnSpace (regarding your use of the Services) ("Notifications"). Please note that your parent or guardian, as well as an administrator from your school and/or district, can view all activity and content associated with your student account, including your Children's Personal Information.
- Your EdLearnSpace account Personal Information or Children's Personal Information is protected by a password for your privacy and security. We also use coding practices which take steps to prevent attack on our Services from web browsers and malicious scripts, by processing all actions through several permission verifications checks.

Terms & Conditions Link: http://www.EdLearnSpace.com/corporate/terms-of-service,
EdLearnSpace Privacy Policy: http://www.EdLearnSpace.com/corporate/privacy-policy

Please return this form once completed.

Student's name:

Parent/Guardian's Name:

I **consent / do not consent** (please circle your choice) to our child's information to be supplied

to:

for the purpose of:

Parent/Guardian's Signature:

Date: