UC SENIOR SECONDARY COLLEGE
LAKE GINNINDERRA

ICT in the ACT Education and Training Directorate

Important Information

Dear Parents/Carers and Students,

To enhance learning opportunities the ACT Education and Training Directorate and thus the College are moving towards creating a more effective wireless network within the College for use by students and staff, as part of this move we will be using a new Virtual Learning Environment (VLE), Google Apps for Education (GAFE).

This new VLE will enable staff to provide support via unit pages for your child's subjects. Student will also have access to Google Docs, an online service which will mean they will never have to worry about losing work again. GAFE is being provided by the Education and Training Directorate in a secure online environment.

During Term 1 2015 we intend that students will be able to access an updated internet service throughout the college. This will allow students to bring and use their own devices or use the devices available at the College to even greater effect in support of their learning.

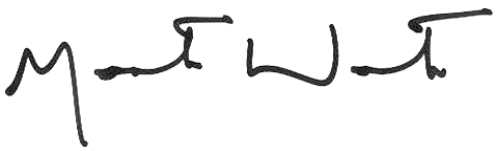
To ensure that you are fully aware of the implications and responsibilities of using own or other devices on the network a number of policies have developed in consultation with the College Board, of which you must be aware.

There are agreements that parents/carers and students need to read, understand and sign before students are able to use the network, their own devices and online software that may be utilised as part of a student's educational program.

I ask that you carefully read the attached policies, sign the relevant agreements and return them to the College as soon as possible. Please be aware that without these signed agreements students will not have access to the network.

If you have any queries please contact the College and we will endeavour to resolve them as quickly as possible.

Yours sincerely,



Martin Watson

Principal
2.2.2015

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

BYOD

Bring Your Own Device

Policy Statement

1.1. UCSSC LG, in consultation with its communities, can allow students to bring their own personal mobile electronic devices to college for the purpose of learning.

1.2. The use of devices at College will be governed by the Colleges guidelines and supporting documents that involve community consultation.

1.3. College-developed guidelines and procedures for BYOD must be communicated to staff, students and parents.

1.4. The use of personal mobile devices at College will deepen learning, will be personalised and student-centred, and will meet the expectations of teachers, students and parents. Prior to implementing BYOD, the College will identify strategies to ensure that all students are able to engage fully in classroom activities.

2. Rationale

2.1. This policy provides a framework for the College that allows students to use personal mobile electronic devices at the College with the capability of connecting to the Directorate's Wi-Fi network.

2.2. The increasing availability of personal mobile devices has accelerated the demand for new models of learning.

2.3. The College is in a position to harness students' connection to their own personal mobile devices for the purpose of developing 21st century learning skills and for fostering digital literacy, fluency and citizenship in a safe environment.

2.4. This policy applies to all ACT Government school staff, 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.

3. School Responsibilities

It is the duty of College to ensure that the College community is aware of their responsibilities under the Communities Online policy and the BYOD policy.

The College should:

- Inform the College community of the existence of these policies.
- Make these policies (and associated guidelines) available to parents/guardians and members of the College community.
- Ensure that students and their parents are aware of, and agree to their obligations under the College's guidelines and procedures, and other relevant Directorate policies.
- Ensure that the College community is adequately informed about the use of the ICT resources within the College community.
- Ensure that College Community is 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.
- Retain a copy of the acceptable use agreements signed and place it on the student's file as a record.

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

The principal will retain the right to determine what is, and is not, appropriate use of PEDs at the College within the bounds of the Directorate's policies and relevant legislation such as the *Information Privacy Act 2014.*

While the Directorate will make every reasonable effort to provide a safe, secure and appropriate online learning experience for the College Community, 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 College 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 College grounds, whether accessing the Directorate network or not, is provisional on the expectation that it complies with the terms and conditions of the Communities Online policy and the Bring Your Own Device (BYOD) in Colleges policy.

Users must comply with Directorate, and College guidelines and procedures, concerning the use of devices at College while connected to the Directorate's Wi-Fi Network.

Mobile phone voice and text, SMS messaging or device instant messaging use by students during College hours is a College-based decision.

Users should not attach any College-owned equipment to their mobile devices without the permission of the College principal or an appropriate staff member.

Users must not create, transmit, retransmit or participate in the circulation of content on their devices that attempts to undermine, hack or bypass any hardware and software security mechanisms that have been implemented by the Directorate or the College.

The College is under no obligation to provide technical support for hardware or software associates with PEDs. The College may choose to provide this service to students if there are sufficient resources available in the College.

Long-term care and support of PEDs

- Students and their parents are solely responsible for the care and maintenance of their devices.
- Students must have a supported operating system and current antivirus software, if applicable, installed on their device and must continue to maintain the latest service packs, updates and antivirus definitions as outlined on the BYOD Student Acceptable Use Agreement.
- Students are responsible for ensuring the operating system and all software on their device is legally and appropriately licensed.
- Students are responsible for managing the battery life of their device. Students should ensure that their devices are fully charged before bringing them to school. The College is not responsible for (or restricted from) providing facilities for students to charge their devices.
- Students are responsible for securing and protecting their device in College, and while travelling to and from College. This includes protective/carry cases and exercising common sense when storing the device. The College is not required to provide designated or secure storage locations.
- Students should clearly label their device for identification purposes. Labels should not be easily removable.
- Students should understand the limitations of the manufacturer's warranty on their device, both in duration and in coverage.

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

BYOD Device Requirements and Student Responsibilities

	Device Requirement	Student responsibility
Wireless Connectivity	The ACT Education and Training Directorate's Wi-Fi network installed in schools operates on the **802.11n 5GHz standard with WPA2 enterprise security**. Devices that do not meet these specifications may not be able to connect.	Student devices are only permitted to connect to the ACT Education and Training Directorate's Wi-Fi network while at school. There is no cost for this service.
Operating System	The current or prior version of any operating system.	Students must ensure they have a legal and licensed version of a supported operating system and of software.
Anti-virus		If applicable, students' devices must be equipped with anti-virus software.
Software and Apps	*List school-based requirements*. All software and apps should be fully updated.	Students should ensure they have the capacity to access Google Apps For Education (GAFE), a good way of doing this is to have google chrome as your browser. GAFE will run in other browsers but please ensure this.
Battery life	A minimum of 5 hours to last the day	Students must ensure they bring their device to school fully charged for the entire school day. No charging facilities will be supplied by the school.
Memory and RAM	A minimum specification of 16GB storage and 2GB RAM to process and store data effectively.	
Hardware Features	Camera and microphone.	
Ergonomics	Reasonable sized screen and a sturdy keyboard to enable continuous use throughout the day.	Students should ensure they are comfortable using devices during the school day particularly in relation to screen size, sturdy keyboard etc.
Other Considerations	Weight: Lightweight for ease of carrying. Durability: Durable and strong.	
Data back-up	Consider a portable hard drive as an appropriate source of back-up storage for essential documents.	Students are responsible for backing-up their own data and should ensure this is done regularly.
Insurance/warranty	Be aware of the terms of insurance policies/warranties for the device. The school will not accept responsibility for loss or breakage.	Students and their parents are responsible for arranging their own insurance and should be aware of the warranty conditions for the device.
Theft and Damage	• Supply a carry case or skin to protect the device that is durable and strong. • Consider a tough and sturdy case to avoid breakage.	Students are responsible for securing and protecting their devices at school. Any loss or damage to a device is not the responsibility of the school or the Directorate.
Maintenance and Support		Students are solely responsible for the maintenance and upkeep of their devices.
Confiscation		Students' devices may be confiscated if the school has reasonable grounds to suspect that a device contains data which breaches the BYOD in School Agreement.

UC SENIOR SECONDARY COLLEGE
LAKE GINNINDERRA

Use of Third Party Web Based Educational Services
Permission from Parents/Guardians

Dear Parents/Guardians,

The University of Canberra Senior Secondary College, Lake Ginninderra 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 the school curriculum.

The use of web based learning resources and cloud based storage have 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 include online content creation, collaborative tools, online educational games and various administrative programs for tracking student assessment data.

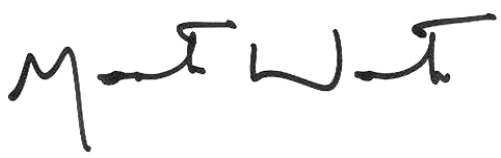
The University of Canberra Senior Secondary College, Lake Ginninderra is registering with a number of web based service providers that require some personal information about a student in your care. I am obliged, under the *Information Privacy Act 2014* to advise you of the reasons for collecting the information, what will be done with it and who else may have access to it.

The below sites have been identified as being a useful component in the teaching programs in many classes at the University of Canberra Senior Secondary College, Lake Ginninderra.

Please indicate your consent/non-consent for each of the services listed by ticking the appropriate option, signing this form and returning it to the school to record on your child's file.

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.

Yours sincerely,



Martin Watson
Principal
2.2.2015

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

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 *Information Privacy Act 2014*It is clearly stated within the this 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 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.

1. **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.

2. **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.
    - It is important that this step is completed explicitly for each separate web service utilised by the school.

3. **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.

4. **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.

UC SENIOR SECONDARY COLLEGE
LAKE GINNINDERRA

Student Privacy Information
Parent Fact Sheet

ACT Government
Education and Training

GOOGLE APPS FOR EDUCATION

Student Privacy Information
Parent Fact Sheet

Google Apps for Education provides students with access to twenty-first century learning tools to support their education, including student email.

This document provides information on the data collected during a student's use of Google Apps and Google's commitment to managing that data.

What data is collected?

Use of Google Apps will mean that student personal information and data will be collected by Google for the purposes of providing the Google Apps services to students. This personal information will include the student's given name, surname, student ID number and all personal information that is contained in a Google Apps service; such as information or data contained in a student's calendar or email (including text, images, photographs, sound and multimedia).

How is the data used?

Google stores and processes personal information solely for the purposes of providing the Google Apps service.

Google scans Gmail to keep its customers secure and to improve their product experience. In Gmail for Google Apps, this includes virus and spam protection, spell check, relevant search results and features like Priority Inbox and auto-detection of calendar events. Scanning to provide product features is done on all incoming emails and is 100% automated.

Google Apps for Education services do not collect or use student personal information and data for advertising purposes or to create advertising profiles.

As part of providing its services, Google may also collect device information, log and location information as detailed in Google's Privacy Policy.

Google will only disclose this data at the direction of the ACT Education and Training Directorate or if compelled to do so by law.

Is the data secure?

Google is committed to protecting the privacy and security of all of their users, including students. Google has strong security systems in place to keep personal information secure, including an encrypted HTTPS connection.

Google's physical data centre access is restricted to authorised personnel and multiple layers of physical security are implemented. Google personnel are only able to access user data in extremely limited circumstances and subject to rigorous approval and oversight.

When is the data deleted?

Unless required by law, Google will delete Customer-Deleted Data from its systems within 180 days of the Department deleting a student's account.

Where is the data?

Google holds user data in its data centres that are located around the world.

Where can I find more information?

Google Privacy Information

Google's approach to privacy, security and transparency with Google Apps for Education is available at

http://www.google.com/edu/privacy

http://www.google.com/apps/intl/en/terms/education_terms.html

https://www.google.com/intx/en/enterprise/apps/terms/dpa_terms.html

http://www.google.com/policies/privacy/

Education and Training Directorate Privacy Information

http://www.det.act.gov.au/functions/privacy

ACT Government
Education and Training

Student Privacy Information
Parent Fact Sheet

ACT Government
Education and Training

MICROSOFT OFFICE 365

Student Privacy Information
Parent Fact Sheet

Microsoft Office 365 (O365) provides students with access to twenty-first century learning tools to support their education.

This document provides information on the data collected during students' use of O365 and Microsoft's commitment to managing that data.

What data is collected?

Users control the information that is transferred to, and stored by, Microsoft in O365. This may include text, images, photographs, sound and multimedia.

In addition, in the course of using the O365 service and in order to deliver the service, Microsoft's systems will generate some information such as logs about user access to the O365 services.

How is the data used?

Microsoft does not use this collected information to track users' online activities or build profiles for behaviour analysis or other commercial purposes.

Microsoft does not use, access or collect this data for any other reason other than to provide the Office 365 services to users - in particular, Microsoft will not use or disclose user data for advertising purposes.

The ACT Education and Training Directorate has ensured through its contract with Microsoft governing the delivery of O365, that there are a number of express commitments relating to user data. These include:

- Ownership of user data rests at all times with users, and not Microsoft.
- Microsoft will meet stringent international standards that are generally acknowledged as the benchmark for providers of Online Services.

Is the data secure?

Physical data centre access is restricted to authorised personnel and multiple layers of physical security are implemented. Microsoft personnel are only able to access user data in extremely limited circumstances and subject to rigorous approval and oversight.

Microsoft use subcontractors to perform a variety of support services for O365. Examples of these include, physical hardware maintenance, technical support and facilities services (eg, security guards at data centre locations).

Microsoft will only disclose data at the direction of the ACT Education and Training Directorate or if compelled to do so by law.

When is the data deleted?

Microsoft will remove all user and associated data from its systems when the Directorate removes a user account from the system.

Where is the data?

For the O365 service, user data is stored predominantly in data centres situated in Hong Kong and Singapore.

Where can I find more information?

Microsoft Privacy Information

Microsoft's approach to privacy, security and transparency with O365 is accessible at

http://www.trustoffice365.com

http://www.microsoft.com/en-us/twc

http://www.microsoft.com/contracts

Education and Training Directorate Privacy Information

http://www.det.act.gov.au/functions/privacy

ACT Government
Education and Training

Please sign and return the following forms

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

Acceptable Use of ICT Statement – Parents/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.

Acceptable Use of ICT Statement – Parent/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 school computers, local applications, and network drives Yes or No:

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

Internet Yes or No: _____

Internal (school) email Yes or No: _____

Google Apps for Education Yes or No: _____

Name of child (printed): ……

Parent and/or Guardian (Name printed): ……..

Parent Signature: …… Date: ……

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

Acceptable Use of ICT Code of Practice for Students

The Acceptable Use of ICT statement for students should be signed by all parents/guardians of students under the age of 18. Students aged 18 and above can sign the form themselves.

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.

The University of Canberra Senior Secondary College Lake Ginninderra has a number of facilities which enable you to access information on computer networks such as the Internet for the purpose of your education. 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 UCSSC Lake Ginninderra.

VIOLATIONS OF THESE RULES MAY RESULT IN

- loss of access;
- legal action if appropriate.

I have read and understood the University of Canberra Senior Secondary College Lake Ginninderra 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: ……..

UC SENIOR SECONDARY COLLEGE
LAKE GINNINDERRA

Acceptable Use of Bring Your Own Device (BYOD) in School Agreement

This BYOD in School Agreement was developed for students of the University of Canberra Senior Secondary College Lake Ginninderra and is consistent with the Directorate's Communities Online policy and Bring Your Own Device (BYOD) in Schools policy.

All Students must read and sign this Acceptable Use of BYOD in School Agreement in the company of a parent unless otherwise directed by the principal.

I agree that I abide by the school's BYOD policy and that ***(please tick)*****:**

- ☐ I will use the Directorate's Wi-Fi network for learning.
- ☐ I will use my device during school activities at the direction of the teacher.
- ☐ I will not attach any school-owned equipment to my mobile device without the permission of the school.
- ☐ I will use my own portal/internet log-in details and will never share them with others.
- ☐ I will stay safe by not giving personal information to strangers.
- ☐ I will not hack or bypass any hardware and software security implemented by the Directorate or my school.
- ☐ I will report inappropriate behaviour and inappropriate material to my teacher.
- ☐ I acknowledge that the school cannot be held responsible for any damage to, or theft of my device.
- ☐ I understand and have read the limitation of the manufacturer's warranty on my device, both in duration and in coverage.
- ☐ I have read the BYOD Device Requirements that form part of this agreement and have ensured my device meets the minimum outlined specifications.
- ☐ I have read the BYOD Student responsibilities that form part of this agreement and agree to comply with the requirements.
- ☐ I understand that I still must honour the terms of the Acceptable use of ICT I signed when using my device.

Student Name: …….. Student ID: …….

Student Signature: ……

In the presence of:

Parent Name: ……

Parent Signature: …….. Date: ……..

Please note this Agreement will be stored on the student's file in the College.

UC SENIOR SECONDARY COLLEGE LAKE GINNINDERRA

Third Party Web Based Educational Services

Provider Details and Information		Consent Provisions
Name of Provider:	**CK-12 Foundation 2015**	
Type of Service:	Online Resources & Training	☐ **Consent**
Website:	http://www.ck12.org/student/	
Student Information Provided:	**email address**	☐ **Non-consent**
Terms and Conditions Link:	http://www.ck12.org/about/terms-of-use/	
Privacy Policy Link:	**http://www.ck12.org/about/technology 2/privacy-policy/**	
Name of Provider:	**Education Perfect**	
Type of Service:	Online Language Learning	☐ **Consent**
Website:	http://worldseries.educationperfect.com//	
Student Information Provided:	**email address, Names, School ID, Classes**	☐ **Non-consent**
Terms and Conditions and Privacy Link:	**http://www.ck12.org/about/terms-of-use/**	
Privacy Policy Link:	**https://start.languageperfect.com/privacy.html**	
Name of Provider:	Google	☐ **Consent**
Type of Service:	Google Apps for Education	
Please see included information for details		☐ **Non-consent**
Name of Provider:	Microsoft	☐ **Consent**
Type of Service:	Office 365, online office suite	
Please see included information for details		☐ **Non-consent**

Please return this form once completed.

Student's Name: ……

Parent/Guardian's Name: ……

…… ……..
Parent/Guardian's Signature Date