



## ICT, Cyber-Safety and Cloud Computing Services Policy

### Cyber-Safety At Findon High School

Last Modified: Monday 3 June, 2019

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of students at Findon High School are based on our core values. To assist us to enhance learning through the safe use of information and communication technologies (ICT's), we are now asking you to read this document and sign the ICT and Cyber-Safety Use Agreement form.

Rigorous cyber-safety practices are in place, which include cyber-safety Use Agreements for staff and students, who have been involved in the development of the agreement. Child protection education, such as the Keeping Safe Child Protection Curriculum, includes information about remaining safe when using new technologies and is provided to all students.

The computer network, Internet access facilities, computers and other ICT equipment and services bring great benefits to the teaching and learning programs at Findon High School, and to the effective operation of the school. The ICT equipment is for educational purposes appropriate to this environment, whether it is owned and/or leased from the school either partially or wholly, and used on or off the site.

The overall goal of Findon High School is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The Use Agreement (ICT and Cyber-Safety Use Agreement) includes information about your obligations, responsibilities, and the nature of possible consequences associated with cyber-safety breaches that undermine the safety of the school environment.

***All students and parents are required to sign and return the consent form. Once the form has been returned to school, students will be permitted to use the school ICT equipment.***

Material sent and received using the Findon High School network and cloud services may be monitored, and filtering and/or monitoring software may be used to restrict access to certain sites and data, including e-mail. **Where a student is suspected of an electronic crime, this will be reported to the police. Where a personal electronic device such as a mobile phone is used to capture images of a crime, such as an assault, the device will be confiscated and handed to the police.**

While every reasonable effort is made by schools and DfE (Department for Education) administrators to prevent student's exposure to inappropriate content when using the department's online services, it is not possible to completely eliminate the risk of such exposure. In particular, DfE cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. DfE recommends the use of appropriate Internet filtering software.

More information about Internet filtering can be found on the websites of the Australian Communications and Media Authority at <http://www.acma.gov.au>, eSafety at <https://www.esafety.gov.au>, the Kids Helpline at <http://www.kidshelp.com.au> and Bullying No Way at <http://www.bullyingnoway.com.au>.

Please contact the Principal, if you have any concerns about your child's safety in using the Internet and ICT equipment and services.



Parents/caregivers play a critical role in developing knowledge, understanding and ethics around their child's safety and safe practices for themselves and the people around them regardless of the time of day. Being cyber-safe is no exception and we invite you to discuss with your child the following conditions to help them stay safe when using ICT at school and outside formal school hours.

**Important terms:**

**'Cyber-safety'** refers to the safe use of the Internet and ICT equipment and services, including mobile phones.

**'Cyber bullying'** is bullying which uses e-technology as a means of victimising others. It is the use of an Internet service or mobile technologies - such as e-mail, chat room discussion groups, instant messaging, webpages or SMS (text messaging) - with the intention of harming another person.

**'ICT equipment and services'** includes computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, portable hard drives, iPods, MP3 players), cameras (such as video and digital cameras and webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), enterprise storage, network switches, routers, printers and any other, similar, technologies both school owned or privately owned. Services include cloud/online based solutions such as, but not limited to Microsoft Office 365, Google Apps for Education (encompassing GSuite) and any FHS service that comprises of electronic communication and/or delivery system, such as DayMap, Wordpress, Papercut, ICT Administration.

**'Inappropriate material'** means material that deals with matters such as sex, cruelty or violence in a manner that is likely to be injurious to children or incompatible with a school or preschool environment.

**'E-crime'** occurs when computers or other electronic communication equipment/devices (eg Internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence.

- 1 I will not use school ICT equipment until my parents/caregivers and I have signed my ICT and Cyber-Safety Use Agreement form and the completed form has been returned to school.
- 2 If I have my own user name, I will log on only with that user name. I will not allow anyone else to use my name.
- 3 I will keep my password private and change it regularly.
- 4 While at school or undertaking a school related activity, I will inform the teacher of any involvement with any ICT material or activity that might put me or anyone else at risk (i.e. bullying or harassing).
- 5 I will use the Internet, e-mail, mobile phones or any other ICT equipment and services only for positive purposes, according to school, DfE and legal requirements, not to be mean, rude or offensive, or to bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke.
- 6 I will only print educational related material.
- 7 I will back up my work to the school network or online drive as well as my removable media. I will not store inappropriate or non-educational material on any network or online drive. IT staff may remove inappropriate material from the network or online drive without notice.
- 8 I will use my ICT devices or mobile phone/s only at the times agreed to by the school & staff during the school day.
- 9 I understand that not all information on the internet is reliable and accurate.
- 10 While at or away from school, I will:
  - access, attempt to access, download, save and distribute only age appropriate and relevant material
  - report any attempt to get around or bypass security, monitoring and filtering that is in place on school ICT equipment and services.
  - not circumvent security, monitoring and alerting mechanisms that the school has implemented.
- 11 If I accidentally access inappropriate material, I will:
  - not show others
  - turn off the screen or minimise the window
  - report the incident to a teacher immediately.



- 12** To ensure my compliance with copyright laws, I will download or copy files such as music, videos, games or programs only with the permission of a teacher or the owner of the original material. If I infringe the Copyright Act 1968, I may be personally liable under this law. This includes downloading such files as music, videos, games and programs.
- 13** I understand that I must not plagiarise. The school has plagiarism checking software and disciplinary action maybe taken.
- 14** Only with permission from the teacher or IT staff will I connect any ICT device to the school network, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/bluetooth technologies.
- 15** I will not put any personal information online. Personal identifying information includes any of the following:
  - my full name
  - my address
  - my e-mail address
  - my phone numbers
  - photos of me and/or people close to me.
- 16** I will respect and treat all ICT equipment and services with care. This includes:
  - not intentionally disrupting the smooth running of any school ICT equipment and services.
  - not attempting to hack or gain unauthorised access to any ICT equipment and services.
  - following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with ICT equipment and services.
  - reporting any breakages/damage to a staff member.
- 17** If I cause deliberate and/or malicious damage to school equipment and/or services, I will incur repair costs.
- 18** The school will monitor traffic and material sent and received using the school's ICT equipment and services. The school will use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.
- 19** The school will monitor and audit its computer network, Internet access facilities, computers and other school ICT equipment and services or commission an independent forensic audit. Auditing of the above items may include any stored content, and all aspects of their use, including e-mail.
- 20** If I do not follow cyber-safe practices, the school will inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. If illegal material or activities are involved or e-crime is suspected, it may be necessary for the school to inform the police and hold securely personal items for potential examination by police. Such actions may occur even if the incident occurs off-site and/or out of school hours.
- 21** I understand that FHS must use my full name to provide a cloud service (e.g. Microsoft Office 365 and Google Apps for Education).
- 22** I understand that LearnLink Office 365, Google Apps for Education and other cloud based services, as deemed appropriate by the school, are only to be used in relation to delivering curriculum objectives, and will not be used to store sensitive, personal or illegal information and/or content.
- 23** I understand that installing and/or accessing any school sponsored software or services (e.g. Office 365 or Google Apps for Education) on my device is at my own risk. I take responsibility for ensuring my files are backed up prior to downloading, installing or accessing any school sponsored software or service.

### **Personal Devices (BYOD – Bring Your Own Device)**

- 24** My privately owned ICT equipment/devices (BYOD), such as a laptop, netbook, mobile phone, USB/portable drive I bring to school or a school related activity, also is covered by the ICT and Cyber-Safety Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment. ICT devices may be examined by the school's monitoring systems and staff.
- 25** I will ensure I have adequate antivirus/anti-malware software on my devices. I will regularly check my ICT devices for virus's and other malicious threats and remove any threats found.



- 26** The Department for Education, SA Government and Findon High School is not responsible for loss/damages to personal devices/mobile devices including applications/information/data stored on, processed or accessed in conjunction with using any provided service.

### **Laptop Programs**

- 27** The school reserves the right to confiscate any device issued through school laptop programs if the conditions of the agreements entered into with Findon High School are broken.
- 28** A Laptop Program device purchased or loaned through the school, may have other applications installed by the user of the device, providing that the software meets the following criteria:
- does not attempt to circumvent security measures or gather information from other devices (snooping, sniffing or other network inspection tools)
  - does not gain unauthorised access to other systems or school ICT infrastructure.
  - is legally obtained. No pirated software or media of any kind is permitted.

### **To the parent/caregiver/legal guardian:**

**Please read this page carefully to check that you understand your responsibilities under this agreement.**

### **I understand that Findon High School will:**

- do its best to enhance learning through the safe use of ICT equipment and services. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on ICT equipment and services at school, or while undertaking school related activities; and enforcing the cyber-safety requirements detailed in Use Agreements.
- respond to any breaches in an appropriate manner.
- provide members of the school community with cyber-safety education designed to complement and support the Use Agreement initiative.
- welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

### **For the Student: My responsibilities include:**

- reading this Cyber-Safety Use Agreement and Cloud Computing policy carefully.
- following the Cyber-Safety conditions and instructions whenever I use the school's ICT equipment and services.
- following the Cyber-Safety conditions whenever I use privately-owned ICT devices on the school site or while undertaking any school related activity, regardless of its location.
- avoiding any involvement with material or activities that could put at risk my own safety, or the privacy, safety or security of the school or other members of the school community.
- taking proper care of school and privately owned ICT equipment and services. I know that if I have been involved in the deliberate and/or malicious damage or theft of ICT equipment and services, I and/or my family/caregiver may have responsibility for the cost of repairs or replacement.
- Bring my device to school every day, full charged and ready for use.
- keeping a copy of this document somewhere safe so I can refer to it in the future.
- asking a staff member if I am not sure about anything to do with this agreement.



## Cloud Computing Services At Findon High School

This policy sets out the terms on which you may access 'Cloud Computing Services' provided by the school, including but not limited to; Google Suite for Education, blogs, LearnLink Office 365 and or LearnLink Office 365 Pro Plus, Adobe Creative Cloud, Freshdesk, Autodesk, Trimble Sketchup, Acer PAT, Naplan, SACE, Unreal, Unity, Microsoft Visual Studio, ViVi, Geogebra. Findon High School reserves the right to sign-up students to other cloud based services for educational purposes. Cloud computing involves the use of internet-based services (rather than a PC or school server) for functions such as email, blogs and data storage.

You will need to sign and return the ICT and Cyber-Safety Use Agreement before you will be allowed to access the Cloud Computing Services.

By signing the ICT and Cyber-Safety Use Agreement, you (including parents/guardians in the case of students under 18 years) are agreeing to the terms set out in this User Agreement, including the consequences of any breach of the terms.

Findon High School will use personal information, such as student's first name and last name to sign up to Cloud Computing Services. The services accessed by the students will have educational value and used as instructed by Findon High School staff.

### Privacy Consent

Information that you transfer or store using the school's Cloud Computing Services may be stored by their respective service providers in the United States of America, or such other country as the cloud service providers may decide. By using the school's Cloud Computing Services, you are consenting to the transfer to, and processing and storage of your information in, such overseas location, even though the privacy laws in those countries may be different to the privacy laws in Australia.

### Acceptable Use

You agree that you will not use the Cloud Computing Services to do anything that is against the law, and that you will not:

- a) give your account password to anyone else;
- b) access (or try to access) anyone else's account, or try to defeat any security controls;
- c) send or help to send unsolicited bulk email (spam);
- d) publish, send or knowingly access material that is pornographic, hurtful or offensive to other people, including material that is defamatory, threatening or discriminatory;
- e) knowingly create or send any viruses, worms, trojans or anything of a similar nature; or
- f) disable, change, reverse-engineer or otherwise interfere with the Cloud Computing Services.

### Monitoring

You agree that IT Support Staff responsible for IT systems will have the ability to (and may at any time) monitor your use of the Cloud Computing Services, including accessing and monitoring any data that you have sent or stored using the Cloud Computing Services, to ensure that you are using the Cloud Computing Services appropriately.

If you notice a problem with the Cloud Computing Services, or if you think that someone is trying to access your account (or someone else's account), you agree that you will tell the school's IT Support Staff immediately.

### Suspension or termination of use and other consequences

If there is an emergency security issue, or if you are suspected of making inappropriate use of the Cloud Computing Services, your access to the Cloud Computing Services may be suspended or terminated. This means that you might not be able to access your school's ICT services, including your school email account. If you are found to have made inappropriate use of the Cloud Computing Services, the school may also apply other disciplinary consequences





## ICT, Cyber-Safety And Cloud Computing Services Use Agreement

We have read and understood this Cyber-Safety Use Agreement and Cloud Computing policy and we are aware of the school's initiatives to maintain a cyber-safe learning environment.

Name of student ..... House Class .....

Signature of student..... Date .....

**For the Parent/Caregiver/Legal Guardian:**

- reading this Cyber-Safety Use Agreement and Cloud Computing policy carefully and discussing it with my child so we both have a clear understanding of our roles in the school's work to maintain a cyber-safe environment.
- ensuring this Use Agreement is signed by my child and by me and returned to the school.
- encouraging my child to follow the cyber-safe strategies and instructions.
- I consent to my child accessing and using cloud based services provided by Findon High School and understand this may include the use of my child's personal information including first name and last name.
- contacting the school if there is any aspect of this Use Agreement I would like to discuss.

Name of parent/caregiver/legal guardian .....

Signature of parent/caregiver/legal guardian ..... Date .....

*Please note: This agreement is required to be signed annually.*

**PLEASE RETURN THIS PAGE TO SCHOOL AND KEEP A COPY FOR YOUR OWN REFERENCE.**