Learning Technologies

User Rights and

Responsibilities Agreement

Contents

USER RIGHTS AND RESPONSIBILITIES

To gain access to any learning technologies on the school grounds, students, parents / caregivers are required to have signed this Learning Technologies User Rights and Responsibilities Agreement. All users are expected to adhere to the following agreement.

1. ACCEPTABLE USE

1.1 Students must take the device to all lessons unless the teacher has requested otherwise.

1.2 Any illegal or offensive material found on a device will result in suspension and/or exclusion from school. Illegal or offensive material includes, but is not limited to, pornographic material, illegally downloaded games/movies/TV series etc. The South Australian Police will be notified regarding any unlawful activity.

1.3 The use of the device is on the understanding that students will follow teacher instructions and access applications and files in safe and ethical ways. Students must not disrupt the smooth running of any school ICT systems nor attempt to 'hack' or gain unauthorised access to any system. The school's wellbeing and Behaviour for Learning processes, and this IT policy, extend outside of school hours and off-site.

1.4 Underdale High School reserves the right to monitor the content of student device and may conduct live monitoring of activity on the device while the device is at school. Students must permit school staff and parents/caregivers to perform checks when requested and may have 'Access Permission/Control' enabled by the school at the school's discretion.

1.5 Teachers and parents/caregivers may recommend a particular student's device has 'Access Permission/Control' features activated, which limit the student's privileges and means they will be unable to install software. These limited privileges may include restricting access to websites, times of day, software and/or applications.

1.6 Consequences for inappropriate use will be in accordance with Underdale High School's Behaviour Support policy and may include confiscation of the device for a period or managed privilege, at the discretion of Learning Area Leaders, Year Level Leaders or other School Leadership staff who will store the device and be responsible for all communication regarding return of the device. Where a student is suspected of any unlawful activity, it will be reported to the South Australia Police.

1.7 At the discretion of the school, a student's device screen may be displayed at any time to staff, students or visitors to the school. Students' screens may be shared on any of the large display screens in the school.

1.8 The camera is only to be used in class with teacher permission. Photos of another person must be with their permission.

2. INTERNET USAGE AT SCHOOL

According to the Department for Education IT Security, Internet Access and Use, and Electronic Mail and Use policies, students may use the Internet only for learning related activities that are approved by a teacher.

They must not cause interference or disruption to other people or equipment, and students may not access or distribute inappropriate material. This includes:

- distributing spam messages or chain letters
- accessing or distributing malicious, offensive or harassing material, including jokes and images
- bullying, harassing, defaming or giving offence to other people
- spreading any form of malicious software (e.g. viruses, worms)
- accessing files, information systems, communications, devices or resources without permission

- using for personal financial gain
- using non-approved file sharing technologies
- using for non-educational related streaming audio or video
- using for religious or political lobbying
- downloading or sharing non-educational material.

While Underdale High School will make every reasonable effort to provide a safe and secure online learning experience for children and students, internet filtering is not 100 per cent effective and it is not possible to guarantee that children and students will not be exposed to inappropriate material.

3. Internet Usage at Home

Internet browsing by students while they are off-site, for example at home, is permitted.

Please note this will not be filtered or monitored by Underdale High School.

Students using their device at home to access the internet must do so in a safe and ethical manner, with parental permission. Parents/caregivers should actively monitor and discuss their child's use of the internet

4. Passwords

Department for Education IT Security and Internet Access and Use policies contain the following main provisions regarding passwords:

- passwords must be kept confidential and not displayed or written down in any form
- passwords must not be words found in a dictionary or based on anything somebody else could easily guess or obtain using person-related information
- students must not disclose their personal passwords to any person other than UHS IT staff or Senior Leadership
- students will be accountable for any inappropriate actions (e.g., bullying, accessing, or sending inappropriate material) undertaken by someone using their personal log-on details.

5. Copyright

Students must be aware of their responsibilities regarding intellectual property and copyright law and ethics, including acknowledging the author or source of information. To ensure compliance with copyright laws, students must only download or copy files such as music, videos or programs, with the permission of the owner of the original material. If students infringe the Copyright Act 1968, they may be personally liable under this law.

6. Printing

Staff and students are encouraged to transmit work electronically and lessen the need to print documents. Students will be permitted to print from all devices. Printing restrictions and charges apply.

7. Software Installation, Games and Music

Students may have Administrator access to their device and may be permitted to install certain types of software and files provided they have acquired a legitimate license. Student installed software must be educational in nature or have a direct relationship to student learning. Non-educational software, games and music are not recommended as they will unnecessarily use space and battery of the device and therefore impede its use for learning. Students using non-educational software, games and files at school will be subject to consequences according to the 'Acceptable Use' section. In instances where the device's performance is restricted due to student installed software and files the device's storage may be erased and by IT Services. Under no circumstances may software and files be installed without the appropriate license. Students doing so will be liable to prosecution.

Parents/caregivers are encouraged to regularly monitor the contents of the device.

8. Social Networking

Under certain circumstances social networking sites may be beneficial for learning. However, in many instances social networking sites can be a distraction and potentially unsafe. Students must seek permission from their teacher or parent/caregiver before accessing social networking sites.

School Internet filters block many (but not all) social networking sites. Parents wishing to filter home internet on the device should refer to the section titled 'Access Permission/Control'.

Students using social networking sites without permission during lessons will be subject to consequences according to the school's Behaviour Support Policy.

Students are reminded to use Cyber-safe strategies and use the Internet in a safe and ethical manner.

9. Access Permission/Control

The devices can be configured with 'Access Permission/Control' capabilities. By default, these are not setup by school. Parents/ caregivers seeking to manage, monitor, and control the time their child spends on the device, including the sites they visit, can contact school IT team for any recommendations as it may involve purchasing a third-party software.

Please note that the implications of turning on 'Access Permission/Control' include:

- the school or parent/caregiver will have an administrator account on the device
- the student will no longer have administrative privileges to the device
- the student will no longer be able to change settings or install software unless the parent/caregiver is present to enter their password – hence the school can only provide limited IT Support in this instance.

10. Private Laptops and Personal Devices

Private laptops and personal devices add complexity to the functionality and maintenance of the school network and are not supported. Only staff, students, and other school-approved users are permitted to access the school's network.

11. Office 365

Office 365 is a service provided for students and supported by the Department for Education for use in schools. This allows Office products to be downloaded onto devices. It also enables collaboration among students on documents, and ongoing backup of student work.

12. Health and Safety

Students are advised to consider the following advice when using their device:

- taking regular rest breaks within the confines of the classroom and at the discretion of the teacher
- working in an environment free from glare
- using the device on a desk rather than on the lap or any soft material as it can block its ventilation which can result in overheat/damage the device.
- angle the screen to minimise the need to bend the neck
- maintaining good posture

13. Cyber-Safety at Underdale Secondary School

Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Underdale School are based on our core values. To assist us to enhance learning through the safe use of Information Technologies (IT's), we are now asking you to read this document and sign the attached Use Agreement Form. Staff, students and parents/caregivers must familiarise themselves with the content of the eSafety Commissioner's Online Safety Book, available at https://www.esafety.gov.au/parents/online-safety-book.

Rigorous cyber-safety practices are in place, which include User 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 IT equipment/devices bring great benefits to the teaching and learning programs at Brighton Secondary School, and to the effective operation of the school. The IT equipment is for educational purposes appropriate to this environment, whether it is owned or leased either partially or wholly by the school and used on or off the site.

The overall goal of Underdale 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 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 will be issued with a User Agreement and once signed consent has been returned to school, students will be able to use the school IT equipment.

Material sent and received using the network 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 South Australia 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 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 , NetAlert at http://www.netalert.gov.au , the Kids Helpline at http://www.kidshelp.com.au and Bullying No Way at http://www.bullyingnoway.com.au .

Please contact Year Level Leader, if you have any concerns about your child's safety in using the internet and IT equipment/devices.

14. Important Terms

'Cyber-safety' refers to the safe use of the internet and IT equipment/devices, 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, social media platforms, instant messaging, webpages, or SMS (text messaging) - with the intention of harming another person.

'School and preschool ICT' refers to the school's or preschool's computer network, Internet access facilities, computers, and other IT equipment/devices as outlined below.

'ICT equipment/devices' includes computers (such as desktops and laptops), storage devices (such as USB and flash memory devices, CDs, DVDs, 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), and any other, similar, technologies.

'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 (e.g. internet, mobile phones) are used to commit an offence, are targeted in an offence, or act as storage devices in an offence

15. Strategies to Help Keep Underdale Students Cyber-safe

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 strategies to help us stay safe when using IT at school and after formal school hours.

15.1 I will not use school IT equipment until my parents/caregivers, and I have signed my User Agreement Form and the completed form has been returned to school.

15.2 If I have my own username, I will log on only with that username. I will not allow anyone else to use it.

15.3 I will keep my password private.

15.4 While at school or a school related activity, I will inform the teacher of any involvement with any IT material or activity that might put me or anyone else at risk (eg bullying or harassing).

15.5 I will use the internet, e-mail, mobile phones or any IT equipment only for positive purposes, 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.

15.6 I will use my mobile phone/s only at the times agreed to by the school during the school day.

15.7 While at 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 at school.

15.8 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.

15.9 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.

15.10 My privately owned IT equipment/devices, such as a laptop, mobile phone, USB/portable drive I bring to school or a school related activity, also is covered by the Use Agreement. Any images or material on such equipment/devices must be appropriate to the school environment.

15.11 Only with written permission from the teacher will I connect any IT device to school IT, or run any software (eg a USB/portable drive, camera or phone). This includes all wireless/Bluetooth technologies.

15.12 I will ask my teacher's permission before I put any personal information online. Personal identifying information includes any of the following:

- my full name/address/phone number
- my e-mail address
- photos of me and/or people close to me.

15.13 I will respect all school IT and will treat all IT equipment/devices with care. This includes:

- not intentionally disrupting the smooth running of any school IT systems

- not attempting to hack or gain unauthorised access to any system
- following all school cyber-safety strategies, and not joining in if other students choose to be irresponsible with IT reporting any breakages/damage to a staff member.

15.14 The school may monitor traffic and material sent and received using the school's IT network. The school may use filtering and/or monitoring software to restrict access to certain sites and data, including e-mail.

15.15 The school may monitor and audit its computer network, Internet access facilities, computers and other school IT equipment/devices 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.

15.16 If I do not follow cyber-safe practices, the school may inform my parents/caregivers. In serious cases, the school may take disciplinary action against me. My family may be charged for repair costs. 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.

DIGITAL LEARNING POLICY USER AGREEMENT

Before being granted access to Underdale High Schools' Information & Communication Technology (ICT) systems, and/or being used with an Underdale High School laptop, students and parent/caregiver(s) must read the Digital Learning Policy with includes the Cyber-safety guidelines, understand its contents and sign and return this Acceptable Use Agreement to the school.

You should keep the Digital Learning Policy for which this agreement applies for future reference

STUDENT AGREEMENT

My responsibilities include:

- Reading this User Agreement carefully
- Following the school's Digital Learning policy whenever I use the school's ICTs
- Following the cyber-safety strategies whenever I use privately-owned ICT devices on the school site or at 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 the school ICTs. I that if I have been involved in the damage, loss, or theft of ICT equipment / devices, I and or my family may have responsibility for the cost of repairs or replacement
- Keeping this document somewhere safe so I can refer to it in the future
- Asking the Digital Pedagogy Leader if I am not sure about anything to do with this agreement

PARENT/CAREGIVER AGREEMENT

My responsibilities include:

- I have read and understood this Digital Learning Policy Use Agreement and discussed 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.
- Contacting the school if there is any aspect of this Use Agreement I would like to discuss.
- I am area that signing and returning this form constitutes a commitment by me, the parent / caregiver to pay such costs and that Underdale High Schools policies relating to the recovery of depts will apply.

Please note that this agreement will remain in force as long as your child is enrolled at this school. If it becomes necessary to add/ amend any information or rules you will be advised in writing.

For further information regarding the device program please email ICT Admin
dl.0965.ictadmin@schools.sa.edu.au

We have read and understood this Digital Learning Policy use Agreement and we are aware of the school's initiatives to maintain a cyber-safe learning environment.

Name of student ______________________________ Home Group__________________

Signature ___________________________________ Date ______________________

Name of parent / caregiver ____

Signature ___________________________________ Date ______________________