



STUDENT AGREEMENT

ACCEPTABLE USE OF LEARNING TECHNOLOGIES POLICY

Access to computers and the schools computing network services are provided for the purpose of teaching and learning. This agreement outlines appropriate use of Unley High School (UHS) and Department for Education networks, computers and students' electronic devices.

Information Communication Technology (ICT) resources are available to all UHS users. The smooth and reliable operation of the school network relies on the appropriate conduct of all users who must agree and adhere to the following agreement.

Access and Security

As a responsible user, I agree to:

- abide by the Unley High School values and will not use material of an offensive, unfair or harassing nature
- access only appropriate and relevant educational material related to teaching and learning
- be accountable for all activity that occurs while I am logged on and not leave workstations unattended with active sessions
- not download excessively large files without teachers' approval
- use all ICT equipment appropriately and report any damage and/or vandalism promptly
- access the school network and other online services, using **only** my own username and password and **never** share these with others
- keep my passwords confidential, and change them when prompted, or when known by another user
- not use passwords that are easily guessed (i.e. use a mix of upper and lower case, use symbols and numbers)
- not disable, interfere with or bypass virus protection, spam and internet filtering, and network security controls
- access only authorised programs and not intentionally download unauthorised software, graphics or music that are not associated with teaching and learning
- ensure that services are not used for unauthorised commercial activities or any unlawful purpose
- never damage or disable computers, computer systems or networks of Unley High School
- not interfere with or use other student's electronic devices
- never knowingly initiate or forward emails or other messages containing:
 - a message that was sent to them in confidence
 - a virus or attachment that is capable of damaging recipients' device
 - chain letters and hoax emails
 - spam, e.g. unsolicited advertising material
- never send or publish:
 - my passwords and user names
 - material regarding illicit drugs or violence
 - hate speech or offensive material
 - material regarding criminal skills and/or illegal activities
 - unacceptable/unlawful material or remarks, including discriminatory content
 - threatening, bullying, humiliating, harassing content or excessive/unreasonable demands upon any person
 - sexually explicit or sexually suggestive material or correspondence
 - information that is false, discriminatory or harassing in nature about a person or an organisation



- promptly tell a staff member (teacher or SSO) if:
 - I suspect I have received a virus or spam (i.e. unsolicited message)
 - I receive a message that is inappropriate or makes me feel uncomfortable
 - another student has accessed the school network and other online services using my username and password
 - another student has accessed the school network and other online services using a teacher's username and password
 - I see anything on a website that is unpleasant or makes me feel uncomfortable
- accept responsibility for my own device(s) at all times
- fully charge any device before coming to school so that it is ready for my school day
- not bring any power chargers and cables from home for use at school
- maintain a regular independent backup of my own files
- follow school processes to connect any device to the school network

I am aware that:

- all use of internet and online communication services can be audited and traced to the network accounts of specific users
- there may be monitoring of my use of school ICT facilities, including what is recorded, and who has access to this information
- the school can, without notice, delete any material found in the school's own storage that is unauthorised, unlawful, obscene, excessive in volume or uncollected for an extended period of time

Privacy and Confidentiality

As a responsible user, I agree to:

- not reveal personal information including names, addresses, photographs, credit card details and telephone numbers of myself or others
- ensure privacy and confidentiality is maintained by not disclosing or using any information in a way that is contrary to any individual's interests. This includes material that is demeaning.
- follow all school cyber-safety strategies, including seeking advice if another user seeks excessive personal information, asks to be telephoned, offers gifts by email or wants to meet a student
- take every precaution to protect school information from inadvertent or malicious public exposure
- not respond to messages, or bulletin boards items that are suggestive, obscene, belligerent, threatening or make me feel uncomfortable

Intellectual Property and Copyright

As a responsible user, I will:

- not plagiarise information and I will observe appropriate copyright clearance, including acknowledging the author or source of any information used
- ensure that permission is gained before electronically publishing users' works or drawings
- always acknowledge the creator or author on any material published
- ensure any material published on the internet or intranet has the approval of the Principal or delegate and has appropriate copyright clearance
- ensure online learner management systems, for example Daymap, Google Classrooms, Moodle, LearnLink and Office 365, are only to be used in relation to delivering curriculum objectives, and will not be used to store sensitive or personal information
- School information must only be stored on school authorised devices. No school or information about another student should be stored on social networking or other external websites such as Google or Facebook





Misuse and Breaches of Acceptable Usage

Students need to be aware that:

- they are held responsible for their actions while using internet and online communication services
- they are held responsible for breaches where they have allowed any other person to use their network and online accounts to access internet and online communication services
- the misuse of internet and online communication services may result in school action which may include, but is not limited to, the withdrawal of access to school ICT facilities, suspension, exclusion and possible referral to SA Police