CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

ICT SERVICES USER AGREEMENT

INTRODUCTION

ICT Services User Agreements are required to be signed by students and parents/caregivers in relation to the use of computers at school and to provide access to ICT services for Personal or Loan devices. This agreement supersedes all previously signed agreements relating to computer use in schools. The agreement will remain in place as long as your child is enrolled at this school.
If it becomes necessary to add/amend any information or condition, you will be advised in writing.
The ICT Services User Agreement must be completed, signed and returned to the ICT Office to enable access to the ICT Services documented in this agreement.

All students in years 2 to 12 are allocated a device or either a Chromebook or Windows Laptop that meets the school minimum specifications. Students are encouraged not to purchase their own laptop to use as a BYO device. This is to protect our network and systems from possible threats to security and integrity. BYOD is permitted at Central Yorke School, however monitoring software and proof of adequate anti-virus protection is mandatory for any device connecting to Central Yorke School infrastructure.

It is an expectation that devices owned by students and brought to school comply with the appropriate legal operating system and software licensing requirements. Private laptops and personal devices add complexity to the functionality and maintenance of the school network. Only school-supplied Laptops, providing they have the standard image applied, can be supported by the school.

Connection to the network will allow access the following:

- Access to the school wireless network
- Limited technical support
- Access to the internet
- Access to printing
- Access to the school's learning management system – Daymap
- Provision of access at no cost to Microsoft Office and OneDrive cloud storage whilst enrolled as a Department for Education student at Central Yorke School

Bringing a device to school and using the school's network is a privilege and not a right and may be revoked by the school.

PERMITTED DEVICES

To assist in teaching and learning, staff are allowed to connect any type of device to the network.
Due to behavioural concerns, students are allowed to only connect a laptop or Chromebook to the school's network. Any attempt to connect their mobile phone or other smart device is prohibited. Use of ear buds or Bluetooth headphones is prohibited, Central Yorke School will provide suitable headphones to help a student should they require them.

ACCEPTABLE USE

Students must take the device to all lessons unless the teacher has requested otherwise. Teaching and learning programs will make use of the device to benefit students' learning through inquiry, collaboration and new ways of demonstrating knowledge.

Off-task behaviour will be subject to consequences in line with school policies.

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

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.

Central Yorke School reserves the right to monitor the content of the 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.

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.

Consequences for inappropriate use will be in accordance with school policies and may include confiscation of the device for a period or managed privilege, at the discretion of sub-school 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.

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.

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

CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

ICT SERVICES USER AGREEMENT

ACCEPTABLE USE

The installation of any unauthorised software, on school devices is strictly prohibited. Many software applications can carry virus and malware threats which can be difficult to detect. This also includes the installation of browser extension games, decorative or personalising software (toolbars etc), any games or media downloading or streaming tools. Under no circumstances is VPN software to be used or stored on school networks or devices. Any software required must be authorised by the ICT manager before installation.

PRINTING

At school, users will be able to print to a printer queue and collect their printing from a nearby printer/print release station via the PaperCut App.

Students and teachers will receive a yearly allocation of funds for printing. Note: students can check they have sufficient credit by viewing their PaperCut account (desktop window) and can request additional funds from the ICT support centre or with their teacher.

BACKUP AND DATA STORAGE

It is the student's responsibility to ensure their data is regularly saved in an appropriate place. The method for saving data is dependent on the device but it is highly recommended that students use the OneDrive cloud storage provided for this purpose. Students are encouraged to use OneDrive for document storage and saving. No guarantee can be made to recover documents that have not been regularly saved or stored locally, plus loss of power or incorrect use of the school device. Students can submit work to teachers using email or Daymap as required.

ICT AGREEMENTS AND PARENT/STUDENT SIGNATURES

ICT Agreements are mandatory for all students from Reception to Year 12 and must be signed at the beginning of each school year before students can access ICT devices.

It is the responsibility of the home class teacher to ensure these agreements are signed and returned as a matter of urgency, preventing disruptions to planned learning activities that require ICT use.

GAMES

The use of games within the teaching and learning program is at the discretion of the teacher. While some games have significant educational benefits, other games have little educational merit and may affect network function.
As a result: All games must be authorised by leadership and ICT, the use of network games or ad-hoc networks is strictly prohibited.

INTERNET USAGE

All Internet usage is monitored and is subject to Department for Education filtering. Inappropriate downloads can be detected when devices are connected to the school's network. While every reasonable effort is made by the school and Department for Education to prevent student exposure to inappropriate content when using the Department's online services, it is not possible to eliminate the risk of such exposure. In particular, the Department cannot filter Internet content accessed by your child from home, from other locations away from school or on mobile devices owned by your child. The Department recommends the use of appropriate Internet filtering software. Any inappropriate use of internet content will be reported, and any activity suspected of being illegal, will be reported to South Australia Police.

USERS AND SECURITY

- Each student has an individual password for logging in to the school network.
- Students are not able to change their allocated password, any changes must be completed via ICT.
- This password cannot be divulged to any other party under any circumstance. Sanctions will be taken against any sharing of passwords.
- ·Any attempt to break into a government computer system is a federal offence carrying strict penalties which are also applicable to minors. Our network audit logs contain information on the user logging in, the computer they are attempting to log in with and various other parameters. This information can, and will be, used to track user access and usage.

CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

ICT SERVICES USER AGREEMENT

WEB 2.0 APPLICATIONS

There are significant educational benefits for some Web 2.0 applications. A Web 2.0 site allows its users to interact with other users. These include web-based communities, hosted services, web applications, social-networking sites, video sharing sites, wikis and blogs. Examples of Web 2.0 apps are Facebook, Spotify, Twitter (X), Reddit, Instagram, Discord, TikTok and Wikipedia. Essentially, Web 2.0 is the internet where users can add content without the need for web designer code etc.

However, many Web 2.0 applications can be unproductive and distracting to student learning. If accessed at home the school will not be liable for any consequences.

Educational Web 2.0 technologies will be used as part of a student's study in various classes. The use of Web 2.0 applications are based on the condition that:

- The technologies, and the use of the technologies, do not breach any ethical and moral issues
- The applications do not distract student learning
- The Web 2.0 technologies are not to be accessed in class, unless specifically directed by the teacher for educational purposes

CLOUD COMPUTING

Google Classroom, Class Dojo, Daymap, Clickview and Office 365, including Office 365 Plus are services provided for students and are supported by the Department for Education for use in schools. These products enable collaboration among students on documents. The Office 365 Service, including Office 365 Plus is only to be used in relation to deliver curriculum objectives, and will not be used to store sensitive or personal information.

Students must ensure they do not upload, access, transfer, process, share, retrieve or display sensitive or personal information, and that they use the cloud service in accordance with the Acceptable Use terms in the General Policy section of this document.

SECURITY AND STORAGE

During the school day when the devices are not being used (for example at lunchtime and during PE etc), the devices should be kept securely locked in the student's locker or in the charging cabinet in the classroom. The device should be properly powered off at the end of the day with all work saved. This will aid to preserve battery life and to prevent heat build-up.

CYBER BULLYING/ELECTRONIC CRIME (E-CRIME)

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways. Cyber bullying is bullying which uses e-technology as a means of victimising others. It is the use of an internet service or mobile technology such as email, chat room discussion group, instant messaging, Webpage or SMS (text messaging) with the intention of harming another person. Examples can include communications that seek to intimidate, control, manipulate and put down or humiliate the recipient. Activities can include flaming (repeated negative messages), sexual and racist harassment, denigration, impersonation, trickery, exclusion and cyber stalking. The targeted person often feels powerless and may need help. Cyber bullying may involve varying levels of severity, ranging from occasional messages to frequently repeated and highly disturbing threats to a person's life. Cyber bullying can therefore be an e-crime, a fact often not clearly understood by those involved. E-crime occurs when a computer or other electronic communication devices (e.g. mobile phones) are used to commit an offence, are targeted in an offence, or act as a storage device in an offence.

Serious breaches of Cyber Bullying and E-Crime are a police matter and will be dealt with through State and Federal laws and South Australia Police.

LAPTOP/CHROMEBOOK AND IPAD ALLOCATION PROGRAM

Each student at Central Yorke School has an allocated electronic device suited to their year level and/or learning level. These devices will be allocated and labelled with the student's name and class. This is the same for any Charging cords, power packs etc if required.

- The school reserves the right to confiscate any device issued through school Chromebook /Laptop programs if the conditions of the agreements entered with Central Yorke School are broken.
- Users who have agreed to use a School Owned Chromebook or Laptop are wholly responsible for always maintaining the device in good repair and condition. Any breakages or wilful damage can be subject to cost recovery and must be reported to ICT Services. Chromebook manufacturing defects are covered by the school warranty.

CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

ICT RESPONSIBILITIES & PLATFORMS

RESPONSIBILITIES WHEN USING COMPUTERS INSTALLED AT CENTRAL YORKE SCHOOL

- Students are expected to care for computers.
- Students have access to computers with the knowledge that the computers are in good care and working order. At the time of use students are required to report operational or damage issues to their teacher and the ICT managers/technicians.
- In the case where a computer/laptop has been provided to a student for in-school use, it is provided in good care and working order and is confirmed at the time. If at any time there are operational or damage issues, your child will report it to the ICT technicians. If the damage is wilful or if the computing device is lost from an unsecured location, parents may be responsible for the full replacement cost of the laptop. School policies related to the recovery of debts will apply.
- If a laptop is damaged or lost by neglect, abuse or malicious act, the principal will determine whether replacement is appropriate and/or whether or not the student retains access to another laptop or other school computing facilities for use. In such cases repair or replacement costs may be passed on to the parent/caregiver for payment. School policies related to the recovery of debts will apply.

NON-SCHOOL APPLICATIONS AND FILES

At all times the performance of computers and laptops is for the primary purpose of student learning. Some software can slow down the performance of the device or corrupt it so that it is unusable. Approval from the IT Network Manager must be sought before loading non-school software. Some software, even if approved for installation, may not be supported by the school. In general restrictions are in place to ensure students cannot install software on the ICT facilities of the school.

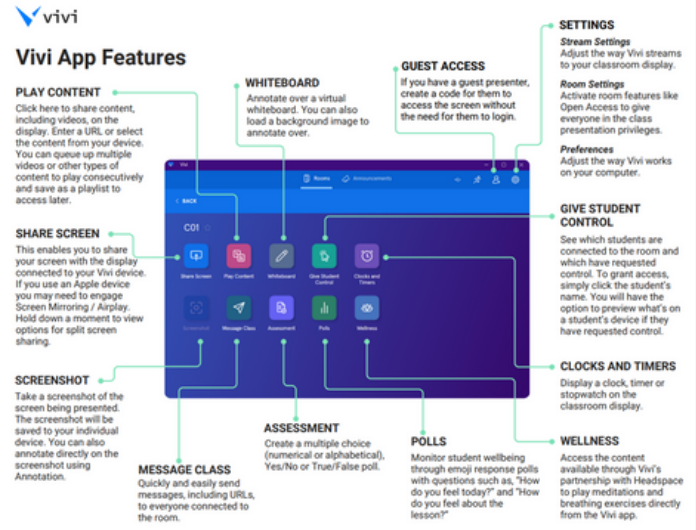
The consequence of contravening school policies on the use of non-school applications will be the restoration of computers and laptops to their original specifications, with the consequential loss of all student data. In addition, other consequences may apply including but not limited to the right of access or use to school ICT equipment being revoked by the school in such circumstances for a period to be determined by the Principal, and or disciplinary measures. It is the responsibility of the student to ensure files related to their learning are backed-up in an alternative location as a matter of good practice.

DAYMAP

Daymap is an all-in-one learning and school management platform designed to streamline communication, planning, and administration in schools.

CYS PAID PLATFORMS AND PROGRAMS

VIVI



What is Vivi?

Vivi is a wireless presentation and collaboration tool that allows teachers and students to share screens, present content, and interact seamlessly with classroom displays.

CLICK VIEW

What is ClickView?

ClickView is a video learning platform that provides access to a vast library of educational content, curriculum-aligned videos, and tools to enhance teaching and learning in the classroom.

To access ClickView, follow these steps:

1. Go to the Website: Visit the ClickView website.
2. Find Central Yorke School: Search for Central Yorke School in the login section.
3. Use Your School Email: Enter your school email address. As we hold the license, you should gain immediate access to the platform.

Important Note: We encourage staff to check if videos are available through ClickView before exploring alternative streaming services or platforms.

CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

DEVICE RESPONSIBILITY & MANAGEMENT CLASSROOM LEVEL

TEACHER RESPONSIBILITY FOR STUDENT DEVICES

Teachers are responsible for monitoring the location and physical condition of student devices.

Daily Device Management:

- If devices are stored in a trolley, conduct a daily stocktake at the end of each day to ensure:
  - All devices are accounted for.
  - Devices are properly charged.

Reporting Issues:

- Any noticeable damage, signs of misuse (e.g., stickers or tampering), or functional issues (e.g., features not working) must be reported promptly to Craig Brennan, our IT Manager via the Sharepoint page.

REPORTING DEVICE FUNCTIONALITY OR SOFTWARE ISSUES

All issues related to the functionality or software of student devices must be reported directly to the IT Manager via the SharePoint Page. Teachers should not attempt to self-diagnose or fix these issues to ensure that software and systems are safely and correctly managed.

Software Management:

- Students require teacher permission to report issues or request software installations.
- It is recommended that teachers send an email request to the IT Manager in advance for any additional software required for student use.

APPS, ADDITIONAL PROGRAMS OR MODIFICATIONS

All requests for apps, additional programs, or modifications must be submitted to ICT with sufficient notice to allow for safe and seamless approval and deployment.
Key Points:

- Prior Approval for Costs:
  - If there is a cost involved, seek approval from your sub-school leader or budget manager before submitting the request to ICT.
- Timely Requests:
  - Provide ample notice to ensure the request can be processed and implemented without disrupting planned activities.

UNACCEPTABLE USE OF ICT DEVICES

Unacceptable use of ICT devices includes, but is not limited to:

- Installation of Unapproved Software: Installing any third-party software that has not been approved by the ICT Department.
- Streaming Services: Only approved platforms such as Spotify, ClickView, ABC iView, and SBS On Demand may be used on-site.
- Personalisation of Devices: Adding stickers, timetables, or other personal items to devices is prohibited. Student names and home classes are managed by the ICT Department.
- Online Gaming: Playing games during school hours or on school devices.
- Inappropriate Content: Accessing, viewing, or searching for inappropriate material, including YouTube content.

The ICT Department strictly monitors device usage. However, it is the teacher's responsibility to remain vigilant and actively supervise students' activities on their devices during class.

Any breaches of acceptable use will result in:

- Notification of class teachers and leadership.
- Consequences such as temporary bans or other disciplinary measures, which will be communicated to both students and parents.

MANAGEMENT OF SHARED ICT DEVICES

Shared ICT devices, such as Specialist Subject iPads and Junior Primary iPads, must be carefully managed to ensure their availability and functionality.
Expectations for Device Management:

- Accountability: All shared devices must be continually accounted for, charged, and returned to their trolley after each use.
- Borrowing Devices:
  - Staff may borrow these devices, but this must be directly negotiated with the specialist area or teacher responsible for them.
  - Devices must be returned immediately after use.

Responsibilities:

- The borrowing teacher is responsible for ensuring the devices are returned in a timely and appropriate manner.
- The specialist area teacher is responsible for verifying that all devices are returned and accounted for.

CENTRAL YORKE SCHOOL

RESPECT - RESILIENCE - RELATIONSHIPS

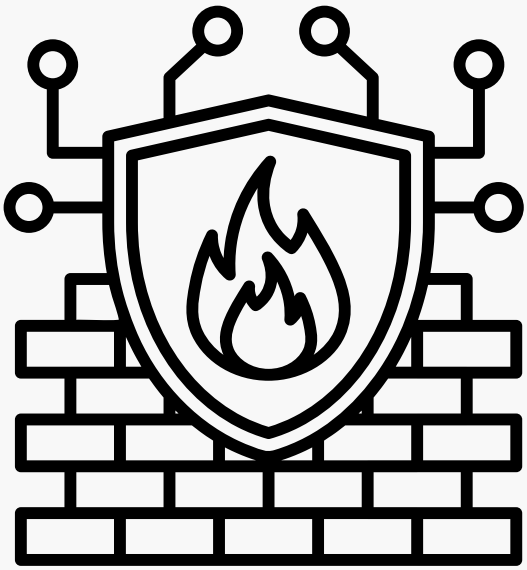
DEVICE RESPONSIBILITY/MANAGEMENT & OFF SITE USAGE

INTERNET USE AND FIREWALL

All internet traffic at the Central Yorke School site is regulated and monitored by a sophisticated firewall program to ensure safe and appropriate use.

Requesting Access:

- Any program, website, or internet-based video that requires bypassing the firewall must be requested via email at least one day prior to ensure timely approval and access.



STAFF AND STUDENT OFF SITE DEVICE USAGE

When using a school device off the Central Yorke School (CYS) network, it is the end user's responsibility to ensure safe browsing habits and appropriate use.

Accessing School Programs Off-Site
Programs such as OneDrive, Daymap, EIK, and EdPass are accessible off-site but require a two-step authentication process for security.

Steps for Logging In Off-Site:

Connect to Personal Internet:

- Ensure you are connected to your own internet.

Browse to the Web Address Required:

- Navigate to the website of the program or platform you need to access.
- When prompted, log in through EdPass.

Troubleshooting Login:

- If you encounter issues, select "Trouble Logging In".
- Click "Select a Different Site", and a search box will appear.

Locate Your Campus:

- Type "Central (Your Campus)" into the search box and select it.

Enter Credentials:

- Use your computer access credentials:
  - Username: Firstname.Lastname
  - Password: Your standard school password.

Two-Step Authentication:

- The system will request a code via SMS.
- Click "Send Code".
- Enter the received code into the provided field and click "Continue".

Access Granted:

- You will be directed to the desired page within the Department system.