



Gawler & District College B-12



# ICT USER AGREEMENT

## CONTENTS

Contents.....	2
Introduction .....	3
ICT Devices .....	4
Appearance and Personalisation .....	4
Cleaning .....	5
Loss and Damage .....	5
Power Issues/Battery/Charging .....	5
Security Procedures .....	5
Data responsibility .....	6
Software, Copyright and Intellectual Property .....	6
Caring for Your Device .....	6
Virus Protection .....	7
Acceptable Use .....	7
Cyber Bullying .....	8
Internet Use .....	8
Email & Spam Filtering.....	9
Cloud Services – O365 .....	9
What is LearnLink Office 365? .....	9
Using LearnLink Office 365 Services .....	10
additional reading.....	11
Cloud Services – GSuite.....	11
What is G-Suite? .....	11
Using G-Suite Services.....	12
Student privacy information summary .....	13
Responsibilities .....	14
Consequences.....	14

## INTRODUCTION

### Dear Parent/Caregiver,

The measures to ensure the cyber-safety of Gawler & District College are based on our core values of Respect, Generosity and Excellence. To assist us to enhance learning through the safe use of information and communication technologies (ICTs), we are now asking you to read this document and sign the attached User Agreement Form.

Rigorous cyber-safety practices are in place, which include cyber-safety 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 ICT equipment/devices bring great benefits to the teaching and learning programs at Gawler & District College, and to the effective operation of the school. The ICT 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 Gawler & District College is to create and maintain a cyber-safety culture that is in keeping with our values and with legislative and professional obligations. The User 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.

This document will act as the User Agreement and once signed and returned to the school, students will be able to use the school ICT equipment.

Material sent and received using the network may be monitored. 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 Department for Education (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, **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**. Gawler & District College recommends the use of appropriate Internet filtering software at home, and connection to the school provided Wifi services whilst at school.

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

Please contact the relevant Middle or Senior Sub-School Leader if you have any concerns about your child's safety in using the Internet and ICT equipment/devices at Gawler & District College.

Any references within this document to the term 'user' will encompass any person or persons accessing ICT resources of Gawler & District College.

## ICT DEVICES

ICT Devices are issued to the user for educational use and remain the property of Gawler & District College. The supply of a device to the user is conditional upon the user's continued association with the College and ongoing agreement and compliance to the terms of usage.

If the student ceases enrolment at Gawler & District College, the device must be returned to the College on the date we specify by notice to you, or on the date the student ceases to be enrolled at Gawler & District College, whichever is earlier. The laptop must be returned to Gawler & District College in good working order, in good repair and if applicable, complete with the AC power adaptor.

Failure to return the device at the allotted time in its original condition will result in Gawler & District College invoicing the student or parents/carers for the repair or replacement cost of the device.

- The device may not be used for commercial purposes.
- The device must remain in Australia and cannot be taken overseas.
- Students are expected to care for loan laptops in relation to transporting, storage and security both on and off-site.
- The type of device provided is determined at the discretion of Gawler & District College based on determining factors such as year level and educational purpose.
- A Device may reference an iPad, Chromebook, Laptop, Desktop or any other digital device provided by Gawler & District College or used whilst onsite.
- Gawler & District College does not give any warranty, representation or assurance as to the quality, fitness for purpose or safety of the device as this is covered by the manufacturer.
- Items/apps provided with and/or installed on devices are subject to review by College staff.
- Devices owned by Gawler & District College periodically check in to our systems to report configuration and management information. The information in these reports may contain but not be limited to the following; Internet provider information, geographical location, IP Address details, installed applications and their usage, Disk usage, plugged in or synchronised devices, battery status, hardware information and internet activity.
- The security and use of the device is the student's responsibility. The student must comply with all directions given by College staff in relation to the use of the device.
- Students must produce the device for inspection whenever requested.
- Personal use of the device is permitted, provided this use does not affect the performance of the device.
- All material on the device is subject to review by College staff and must meet all acceptable use criteria.
- Gawler & District College may lock or disable the device at any time
- Students are not permitted to change device specifications, make modifications, add upgrades, or attempt to access the device internals.

## APPEARANCE AND PERSONALISATION

- As the devices are the property of the College, they are not to be altered or personalised in any way that is not completely irreversible. No labels or stickers are permitted (excluding those applied by Gawler & District College)
- The device will be permanently marked with identifying information as required by the Department for Education Guidelines. Additionally, labels containing the Asset Tag Number and student name will be attached.

**These labels must not be removed.**

## CLEANING

- To clean your device or its screen:
  - Switch off your device
  - Lightly dampen a non-abrasive cloth with water and gently wipe the screen in a circular motion.
  - Use a microfiber cloth to gently dry off any remaining residue
- **Do not directly apply water or cleaner to the device or its screen**

## LOSS AND DAMAGE

- Warranty on devices covers normal defects and usage issues. It does not cover negligence, abuse, malicious damage or loss.
- It is the student's responsibility to take appropriate precautions to prevent wilful damage or theft.
- In the case of loss or damage as a result of negligence, abuse or malicious act the student or the parents/carers will be responsible for meeting the cost for repairs or full replacement of the device.
- Device screens are delicate and will be damaged if poked, prodded, pushed or slammed.
- Any instances of vandalism, damage, loss or theft must be reported immediately to the College. In the case of a suspected theft a police report must be made by the family and an event number provided to the College.
- Parents/carers will be required to replace lost or damaged chargers.
- Neither the student nor their family members must try to sell any College device, offer the device as security or give possession of the device to anyone else.
- Parents may choose to evaluate their personal home contents and car insurance to cover equipment on loan to their child in the event of loss or damage while in the care and custody of the child.
- In instances where damage or loss has occurred involving students other than the student it has been assigned to, the incident will be further investigated.
- In the case of accidental loss or damage a witnessed statutory declaration signed by the parent/carer should be provided.
- If a device is damaged or lost the Deputy Principal will determine whether replacement is appropriate and/or whether or not a student retains access for home use, if applicable.

## POWER ISSUES/BATTERY/CHARGING

- The battery can be conditioned to ensure a long life.
  - It should be fully charged whilst the device is powered off
  - Use the device without recharging until it powers itself off
  - Repeat this process 2 times
- Devices can be used with the AC charger attached where power sockets are safely available
- Year 8 to 12 Students are able to take the device home but must bring the device to the College fully charged each day. Classrooms may have limited facilities to recharge devices.

## SECURITY PROCEDURES

- **Do not leave your device logged on when you are not using it.** It is strongly recommended that you secure your device with a password protected screensaver or pin code. This locks your device after a set period of inactivity, reducing the risk of someone else performing any actions using your digital identity.
- You must update software with security patches when they are released. This occurs automatically whenever your laptop is connected to the College network, notifications may offer early adoption of required updates.

- During a school day when the device is not being used and the student is unable to keep the laptop on them (e.g. at lunchtime, during PE etc), the device should be securely stored in the classroom or designated storage area.

## DATA RESPONSIBILITY

- Information stored ON the device is not backed up by ICT systems.
- Gawler & District College provides network and cloud storage facilities for daily use and or backup locations, network storage is regularly backed up by the College.
- In the event of failure, our College IT technician(s) may be able to restore your device to its original state. There is no guarantee that data stored on your device can be recovered. Before installing new software, ask first for assurance and make sure your backups are up to date.

## SOFTWARE, COPYRIGHT AND INTELLECTUAL PROPERTY

- Each device will be loaded with Gawler & District College approved applications (apps) configured for use on the College network.
- Where applicable, this will include anti-virus software, Microsoft, Apple and Google apps.
- Software installed by the College is copyright and must not be distributed or deleted without written permission from the College.
- While some games have significant educational benefits, other games have little educational merit and may affect network function. As a result:
  - The use of any non-College supplied games is banned
  - No ad-hoc networks are to be formed.

## CARING FOR YOUR DEVICE

- For extra protection, always pack your device in a protective cover if you are carrying it from one place to another or in your College bag.
- Do not remove a cover from an iPad unless directed to do so.
- Do not wrap the cord too tightly around the power adapter or the cord will become damaged.
- You still need to be careful with a device whilst it is in your bag.  
**Do not drop the bag from your shoulder. Always put your bag down gently.**
- Laptops should be shut down before being placed into a protective cover.
- Avoid exposing your device to:
  - Direct sunlight or sources of heat such as desk lamps or a hot car
  - Dust, dirt, rain, liquids or moisture
  - Heavy shock or vibration.
  - Avoid applying pressure to the screen of any device.
  - **Do not store your device in the same place as a water bottle or any container holding liquid.**

## VIRUS PROTECTION

For applicable devices the following applies:

- Anti-virus software and monitoring software may be loaded onto the device during the initial processing of the device. Updates of this software may be scheduled at various times.
- Students should ensure that any anti-virus software and all other updates are kept up-to-date on their device.
- Internet traffic is automatically scanned for viruses when connected to the College network.
- Students that have the right to personally use their device, and connect to the Internet from home are required to take all steps to protect the device from virus attacks.
- You must not install any additional antivirus software as this can cause conflict with existing Antivirus software
- Viruses can enter laptops through:
  - Removable media such as CDs, DVDs and USB memory sticks
  - E-mails
  - The Internet (including web browsing, FTP/Torrent programs and chat programs/rooms).
- **Helpful Tips**
  - Do not open any files attached to suspicious or unknown emails
  - Do not click on any links in suspicious emails or from unknown senders
  - Exercise caution when downloading files from the Internet. Save the files to the laptop's hard disk and run the virus scanner on the files before opening them
  - Delete chain and junk emails. Do not forward or reply to any of these
  - Never reply to Spam
  - Hundreds of viruses are discovered each month. Run your virus scan regularly
  - Avoid indiscriminately loading non-standard software onto the laptop as it can result in an infection by viruses and spyware which are a common cause of laptop failure.

## ACCEPTABLE USE

The College ICT Team maintain devices and network infrastructure so that they operate reliably and effectively, ensuring that the resources needed are available for all users. The following guidelines are outlined to ensure all users are able to access the latest technology in an acceptable and safe learning environment.

- Users will avoid websites with content that is violent, racist, sexist, pornographic, dominated by offensive language and/or illegal in any way
- Do not engage in cyber bullying or e-crime
- Under privacy legislation it is an offence to take photographs of individuals without their expressed permission and place these images on the Internet or in the public forum
- No device with camera capabilities is to be used in change rooms or toilets
- Passwords should remain confidential. No user should log-on another student using their password
- Engaging in chat websites or downloading files is not permitted unless forming part of a legitimate class activity guided by the teacher of that class
- The Federal Communications Act determines guidelines for appropriate use. Inappropriate use of the internet and email is a serious matter and can have significant consequences, e.g. sending a message over the internet using someone else's name.
- It is the responsibility of students to maintain sufficient credit in their printing accounts to allow subject related tasks to be carried out.
- Do not name files, folders, aliases or applications inappropriately with content that is violent, racist, sexist, sexual, or provocative.

- Do not bring in to the College, or use, games or any other materials which may be offensive to others
- Circumvention, bypassing or disabling of monitoring, recording or administrative systems is prohibited. Some of these systems or services may include but not be limited to; proxy bypass technologies, VPN/TOR networks, websites designed to download content from filtered websites
- Circumvention of, or disconnection from, the Gawler & District College WiFi service whilst on site is prohibited, this includes 'hotspotting'
- Any privately owned / personal device brought to Gawler & District College is also subject to the Acceptable User Agreement
- LearnLink Office Applications, including Office 365 Pro Plus, are only to be used in relation to delivering curriculum objectives, and must not be used to store sensitive or personal information

## CYBER BULLYING

E-technology provides individuals with a powerful means of communicating instantly with others in both positive and negative ways.

By definition, 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 social media, email, online chat, instant messaging, web pages or SMS (text messaging) with the intention of harming another person. Examples of cyber bullying include but are not limited to, communications that seek to intimidate, control, manipulate, put down or humiliate the recipient.

Any form of cyber bullying or e-crime will be dealt with through the College's policies.

Serious breaches are a police matter and will be dealt with through State & Federal laws and SA police.

## INTERNET USE

- Users can access the Internet via the College's network while on-site. Access will be monitored and subject to strict filtering.
- Attempts to bypass internet filtering and/or using Torrent websites will result ICT restrictions.
- Users are responsible for the content that their internet account accesses.
- Users are to only connect to the internet using their own user account.
- All internet access on the College's network is recorded and logged outside of the device.
- Offsite internet usage of the school provided device may be recorded.
- Gawler & District College is not responsible for any materials viewed on networks that are external to the College.
- Gawler & District College is not responsible for any data charges incurred by the use of a supplied device on networks that are not provided by the College. Some data usage may occur during information gathering/reporting/update procedures above and beyond normal consumption.
- All school email accounts and on site internet activity will be actively monitored for keywords and filters will prevent and/or report on inappropriate messaging and/or web searching where possible. This will include but may not be limited to categories such as:
  - Drugs
  - Self-Harm
  - Predatory
  - Religious Slurs
  - Racism
  - Sexual or Gender Slurs
  - Profanity
  - Aggression

## EMAIL & SPAM FILTERING

Gawler & District College students are provided with a Learnlink email address

Emails can be accessed anywhere with an internet connection, this can be done by accessing

<https://www.learnlink.sa.edu.au>

The Department for Education provides a spam e-mail filter service for all users, however in some instances spam email can reach us. Staff and students are requested to report spam to ICT support via email to

[dl.0774.icatadmin@schools.sa.edu.au](mailto:dl.0774.icatadmin@schools.sa.edu.au)

A user is not to use the school or departments email systems for spreading/sending/distributing spam e-mail.

## CLOUD SERVICES – O365

Gawler & District College will utilise the expanded email service offered to students with additional services, and will be known as LearnLink Office 365.

LearnLink Office 365 is a customised package of Microsoft Office 365, tailored for the South Australian public education system, and is offered at no additional charge to parents/guardians whilst their student remains enrolled at Gawler & District College.

Users at Gawler & District College will be able to download licenced versions of common Microsoft applications used in teaching and learning at no charge, for use on their device regardless of an internet connection. They will also have their own online storage space for files that can be shared with other students and teachers.

Below is some important information regarding the LearnLink Office 365.

## WHAT IS LEARNLINK OFFICE 365?

LearnLink Office 365 provides students with an email and collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of their educational program.

All data and information within LearnLink Office 365 is stored within an Australian based 'cloud' and provides the following services to students.

- **Office 365 ProPlus**

Office 365 ProPlus provides the latest versions of Microsoft Office applications for desktop PCs, Macs and mobile devices, including Windows, iOS and Android devices.

Office applications include Word, Excel, PowerPoint, OneNote, Access, Publisher and Outlook, however not all Office applications are available for Mac, iOS and Android devices.

Office applications can be installed, via the internet, on up to 5 personal computers and up to 5 mobile devices owned by a student (including parent-owned). Once installed, the applications can be used without an internet connection. Periodic internet connection is required for accessing data stored in cloud services, updates and licencing via your LearnLink Office 365 account.

- **Office Online**

Office Online is a web based, lightweight version of Microsoft's Office productivity suite (including Word, PowerPoint, Excel, and OneNote) that can be used on most devices capable of connecting to the internet via a web browser.

- **OneDrive for Business**

OneDrive for Business is a cloud service where students can store, sync, update, and share files from any internet connected web-browser, and collaborate on Office documents.

Each student will receive 1 Terabyte (or 1000 Gigabytes) of storage space in Microsoft's Australian cloud. By default, all data and files are private, however they can be shared with other LearnLink Office 365 users, including staff and students of other schools and preschools, but not anyone external to DfE schools/preschools.

## USING LEARNLINK OFFICE 365 SERVICES

A number of services provided by LearnLink Office 365 require internet access. When students are onsite internet access will be filtered by the College however access from home/off-site is not filtered by the College and as such should be supervised.

Please be aware that as with any internet use, it is possible (although unlikely) that viruses and/or other malicious software could be introduced to your personal computing devices via LearnLink Office 365 services (including email).

**It is strongly recommended personal devices have suitable anti-virus / anti-malware software installed and regularly updated, and the device operating system is regularly updated.**

Users of LearnLink Office 365 are responsible for the information/data in their LearnLink Office 365 account and any important information should be backed up. LearnLink Office 365 including Office 365 ProPlus is only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive or personal information.

### INSTALLING OFFICE 365 PROPLUS

Office 365 ProPlus applications will need to be installed on a computer or mobile device (personal device) before it can be used.

Although unlikely, it is possible that installing Office 365 ProPlus on your personal device may cause problems, such as conflicts with other software you have installed.

It is recommended that you:

- Backup your personal device, prior to installing Office 365 ProPlus application(s); and
- Ensure your personal device meets or exceeds the Office 365 System Requirements

<https://products.office.com/en-au/office-system-requirements>.

### WHAT IF I DO NOT WANT MY CHILD TO ACCESS LEARNLINK OFFICE 365 SERVICES?

The school / preschool requires written notification if you do not consent to your child using the additional LearnLink Office 365 Services. Please email dl.0774.ictadmin to notify the school.

### HOW WILL MY CHILD ACCESS LEARNLINK OFFICE 365 SERVICES?

LearnLink Office 365 services can be accessed by students via [www.office.com](http://www.office.com) and signing in with their Learnlink account details. They can also access Office 365 apps via a link on the Learnlink email page:

<http://www.learnlink.sa.edu.au>.

Instructions for O365 access are downloadable from our website:

<https://www.gdc.sa.edu.au/our-programs/ict-services/>

## ADDITIONAL READING

More information about Internet safety can be found here:

Australian Communications and Media Authority - <http://www.acma.gov.au>

Kids Helpline - <http://www.kidshelp.com.au>

Bullying No Way - <http://www.bullyingnoway.com.au>

**Please contact the relevant Middle or Senior Sub-School Leader, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.**

## CLOUD SERVICES – GSUITE

Gawler & District College will utilise the Google G-Suite for education and offer some of its services to students, these services will be known as G-Suite (formerly Google Apps).

G-Suite is a customised package of Google products, tailored for the South Australian public education system, and is offered at no additional charge to parents/guardians whilst their student remains enrolled at Gawler & District College.

Students at Gawler & District College will be able to use Google alternatives to Microsoft applications used in teaching and learning at no cost, some classes will use these products at the core of their teaching and learning. Some programs may be used without an internet connection. They will also have their own online storage space for files that can be shared with other students and teachers within the school and moderators where required.

To provide and encourage a safe learning environment Gawler & District College has turned off access to the email (Gmail), chat (hangouts), and social (G+) components of G-Suite. Students will use their school provided email account in place of these services. Gawler & District College will continue to monitor and enable or disable G-Suite services that become available in the future in line with maintaining a safe learning environment for our students.

## WHAT IS G-SUITE?

G-Suite provides students with a collaboration platform to create and/or upload/share content. This may include websites, presentations, written, audio, images and video material as part of their educational program.

All data and information within G-Suite is securely stored in geographically distributed data centres as a 'cloud' and provides the following services to students.

- **Google Docs / Sheets / Slides**

Available anywhere any time on any device students will be able to access their work to submit, change or review. Collaboration features will enable real time commenting and editing with peers on the same document.

Similar to Office Online and Microsoft products such as Word, Excel, and PowerPoint. These applications provide students flexible and friendly alternatives that integrate with the G-Suite experience

With revision history and automatic saving, work entries can be easily followed, reversed, or restored. Work is saved continuously as editing occurs to allow students to continue on where they left off on another device; the right tool for the right job at the right time.

Docs/Sheets/Slides can operate in offline mode for creating new files or files that have been flagged for offline use. There is no limit to the number of devices or locations that can be used to access content.

- **Google Classroom / Forms / Sites**

With Google Classroom and Google Forms, classes can be created to distribute assignments, give quizzes, send feedback, produce a survey and see everything in the one place. Sites provides a simple way to produce websites that can be shown to peers without leaving the safety of the school community.

- **Google Drive**

Google Drive is a cloud service where students can store, sync, update, and share files from any internet connected web-browser, and collaborate on Google documents. It can be used like a virtual storage device to transfer files and folders between computers including backups.

Each student will receive unlimited storage space in G-Suite's cloud. By default all data and files are private, however they can be shared with other Gawler & District College approved G-Suite users, including staff and students of other schools and preschools, but not anyone external to DfE schools/preschools.

## USING G-SUITE SERVICES

A number of services provided by G-Suite require internet access. When students are onsite internet access will be filtered by the College however access from home/off-site is not filtered by the College and as such should be supervised.

Please be aware that as with any internet use, it is possible (although unlikely) that viruses and/or other malicious software could be introduced to your personal computing devices via G-Suite services.

It is strongly recommended personal devices have suitable anti-virus / anti-malware software installed and regularly updated, and the device operating system is regularly updated.

Users of G-Suite are responsible for the information/data in their LearnLink Office 365 account and any important information should be backed up. G-Suite is only to be used in relation to delivering curriculum objectives, and must not be used to store, transmit or share sensitive or personal information.

### G-SUITE OFFLINE ACCESS

G-Suite applications can be installed on a computer or mobile device (personal device) for offline use.

Although unlikely, it is possible that installing G-Suite on your personal device may cause problems, such as conflicts with other software you have installed.

It is recommended that you backup your personal device, prior to installing Docs, Sheets, Slides or Drive application(s).

To install G-Suite in offline mode follow the google support article; <https://support.google.com/docs/answer/6388102>

### WHAT IF I DO NOT WANT MY CHILD TO ACCESS G-SUITE SERVICES?

The school / preschool requires written notification by if you do not consent to your child using the G-Suite Services. Please email [dl.0774.ictadmin@schools.sa.edu.au](mailto:dl.0774.ictadmin@schools.sa.edu.au) to notify the school.

### HOW WILL MY CHILD ACCESS G-SUITE SERVICES?

G-Suite services can be accessed by students by logging in with their Learnlink email address and password.

### ADDITIONAL READING

More information about Internet safety can be found here:

Australian Communications and Media Authority - <http://www.acma.gov.au>

Kids Helpline - <http://www.kidshelp.com.au>

Bullying No Way - <http://www.bullyingnoway.com.au>

**Please contact the relevant Middle or Senior Sub-School Leader, if you have any concerns about your child's safety in using the Internet and ICT equipment/devices.**

### WHERE WILL INFORMATION/DATA BE STORED?

LearnLink Office 365 service is a Cloud based service, meaning it can be accessed from any Office 365 compatible internet connected device anywhere/anytime. All the information and data is stored in Microsoft's Australian data centres and is subject to Australian Privacy Laws, regulations, and standards.

G-Suite offers the similar Cloud based services as LearnLink Office 365 however the servers are operated under United States law. The location of data for G-Suite is within Google's network of geographically distributed data centres. More information can be found here:

<https://www.google.com/about/datacenters/inside/locations/index.html>

### WHAT INFORMATION AND DATA WILL BE COLLECTED?

Learning materials used by educators to teach the student, and information/data created or uploaded by the student in the LearnLink Office 365 and G-Suite services will be stored in the data centres. This may include text, images, photographs, sound and multimedia (e.g. videos).

Microsoft and Google does not access, use, track or collect information or data about the student, other than to deliver the Office 365/G-Suite service on behalf of The Department for Education. In doing so, some system generated data is logged, such as who accessed the services and when.

### WHO HAS ACCESS TO MY CHILD'S INFORMATION AND DATA?

The student owns and controls the information and data they create or upload to the LearnLink Office 365 and/or G-Suite service. They can share their information and data with other LearnLink Office 365 or G-Suite users of the same platform; this includes staff and students from other DfE schools or preschools. Anyone external to DfE is unable to access student information and data.

Processes are in place to allow authorised DfE staff to access information and data the student has created or to uploaded to the service where required.

Microsoft will only disclose information and data at the direction of DfE or if required to do so by law. Google will only disclose information and data with direct requests from government and actively pursues limiting the amount of supplied information to only that which is required

### HOW SAFE IS STUDENT INFORMATION AND DATA?

Microsoft Office 365 Service (LearnLink Office 365) has been [certified by the Australian Government](#) as safe to use for government information. The certification letter and report has been verified by DfE. Additionally Microsoft's Office 365 Service is certified to several international security standards.

Google G-Suite for education has a strong security and privacy focus with respect of these two elements being a core priority of Google. More information can be found at the following websites.

Google Cloud Trust: <https://support.google.com/googlecloud/trust/?hl=en>

G-Suite Security: <https://gsuite.google.com/security/>

## RESPONSIBILITIES

### **Gawler & District College will:**

- Do its best to enhance learning through the safe use of ICT. This includes working to restrict access to inappropriate, illegal or harmful material on the Internet or on school ICT equipment/devices at school, or at school related activities; and enforcing the cyber-safety requirements detailed in the ICT Use Agreement.
- Respond to any breaches in an appropriate manner and as directed by school leadership and or principal
- Provide members of the school community with cyber-safety education designed to complement and support the Use Agreement initiative.
- Store a current version of this document in accessible locations.
- Welcome enquiries at any time from parents/caregivers/legal guardians or students about cyber-safety issues.

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

- Reading this ICT Use Agreement carefully.
- Following the cyber-safety strategies and instructions provided by my teachers and this Use Agreement whenever I use the school's ICT equipment and devices. This also applies to privately owned devices when using them at school.
- Logging on to devices only using my own username and password
- Keeping my passwords private
- Informing a teacher about any 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
- Showing a teacher, but not showing other students, if I accidentally access inappropriate material
- Using the Internet, e-mail, or any ICT device only for positive purposes. I will not be mean, rude or offensive, or bully, harass, or in any way harm anyone else, or the school itself, even if it is meant as a joke
- Respecting and taking proper care of school ICT equipment.
- Storing only files related to my learning in my network folder or in the cloud
- Not providing personal details online, such as your full name, address, phone number or photos
- Not attempting to hack, disrupt or gain unauthorised access to any school system
- Not attempting to bypass website filtering
- Asking the home group teacher if I am not sure about anything to do with this agreement.

## CONSEQUENCES

- Where there is a contravention of this ICT Use Agreement, consequences will include any or all of the following dependant on severity:
  - Resetting any ICT device on loan, which may result in the loss of data if back-ups have not been kept up to date.
  - Locking or disabling of a loan device from accessing the school infrastructure
  - Deletion of inappropriate files and or folders and/or unapproved software
  - Disabling/suspension of ICT user account
  - The school may inform my parents/caregivers. In serious cases, the school may take disciplinary action. My family may also be charged for replacement or 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

Other sanctions may be imposed as appropriate and determined in consultation with College Leadership and the Principal.