Government of South Australia
Department for Education

LUCINDALE AREA SCHOOL
School and Community Working Together

ICT AND CYBER SAFETY HANDBOOK

Applicable to Senior Students

Introduction

The purpose of this handbook is to outline the policies and procedures for the effective use of Information and Communication Technology (ICT) resources within our school community. These guidelines ensure that all students, parents, and staff are informed of their roles and responsibilities, fostering a safe and productive ICT environment.

It encompasses:

- The Laptop Program, which provides essential information on device use and features.
- Cyber safety principals for online behaviour and interaction.
- Acceptable use policies for ICT equipment and internet access.

Laptop Program

Ownership and Models

Students from Year 7 onwards are encouraged to participate in our school Laptop Program. Families have the option to own, loan, or borrow school-approved laptops. Ownership details depend on the option chosen, with specifications meeting educational needs.

Cost and Purchase Guidelines

Since 2022, Lucindale Area School's Laptop Program has provided families with a streamline approach to acquiring school approved laptops. The school sources a specific laptop model and offers parents the flexibility to purchase the device outright or through a payment plan of up to three (3) years.

By standardising the laptop model, the program ensures a consistent platform for all students, offering the following benefits:

- Purchased or hired devices can be taken home, pre-installed with all required software.
- Each device comes with a three-year warranty for peace of mind.
- Software licensing is covered under Department for Education (DfE) agreements.
- On-site device management and support are included, with access to "hot-swap" loan devices during repairs.
- Standardised models ensure seamless connectivity to the school's wireless network.

What's Included in the Cost:

The purchase price of the laptops covers:

- Infrastructure upgrades
- Technical support
- Accessories
- Warranty
- Software

Loan and Borrow Options

For students who do not purchase a laptop, the program offers flexible alternatives:

- A term-based hire of a school device.
- Daily borrowing of older but fully functional laptops.

Device Specifications

The laptops provided through the program are carefully selected to meet the school's requirements and to ensure consistency in quality and functionality. Key specifications and guidelines include:

- All laptops are pre-installed with the required software for classes, including access to online textbooks and tools necessary for the curriculum.
- These devices are fully supported by the school for technical and software-related issues.
- To comply with Workplace Health and Safety (WHS) guidelines, devices cannot be charged in the classrooms. Students must ensure their laptops are fully charged before arriving at school.
- Students are strictly prohibited from altering device specifications, installing modifications, or adding personal upgrades.
- **Important:** Any attempt to change hardware components will void the manufacturer's warranty.

Issuing and Preparation of Devices

Before laptops are issued to students:

- Parents/Carers must choose an option and sign the relevant agreement form, acknowledging the programs terms and conditions.
- Each laptop will be imaged with the authorised school software configuration and registered in the school's database. This registration includes a unique identifier linked to the student.
- Students are required to bring their laptops to school every day, fully charged and ready for use.

End of Lifecycle

The laptop remains the property of the school for the duration of the signed agreement. Once all laptop fees have been paid, ownership of the device will transfer to the student.

Before leaving the school, students are required to bring their laptops to the ICT desk in the Library. The School's software image will be removed as part of the off-boarding process. This step restores the device to factory settings, and **all data stored on the laptop will be permanently erased.**

Once a student is no longer enrolled, the laptop will not allow sign-in until the school's software image has been removed.

To avoid data loss, students must ensure that any important files are backed up to the cloud or an external storage device before handing the laptop in.

Insurance and Warranty

Laptops purchased through the school include a standard three-year (3) manufacturer's warranty. This warranty covers manufacturer defects and issues arising from normal use. However, it **does not cover** damage caused by:

- Negligence
- Abuse
- Malicious acts
- Accidental damage (e.g. cracked LCD screens)

Non-Warranty Damages:

Students are responsible for any loss, theft, or damage that is not covered under the manufacturer's warranty, including incidents occurring at home or during travel to and from school.

Additional Insurance Coverage:

It is strongly recommended that families add the laptop to their household insurance policy or take out separate accidental damage, theft, or loss coverage to safeguard against non-warranty incidents.

Elements of this Policy and Procedures booklet apply depending on the ownership structure.

Acceptable ICT & Cyber Safety Policies

Student Responsibilities

Students are entrusted with the care and proper use of the school's computing resources. It is their responsibility to handle all ICT devices carefully and use them constructively to support their learning. Misuse or neglect of these resources undermines the shared learning environment.

To meet these responsibilities, students must:

- Log in to the school network using only their personal account credentials.
- Never tamper with device settings, hardware, or connections (e.g., switches, buttons, or cables) unless explicitly authorised by a teacher.
- Leave all equipment in its designated location unless they have specific permission from a teacher to move items.
- Report any equipment malfunctions or issues to the appropriate school staff promptly.
- Ensure laptops and other devices are brought to class fully charged and ready for use.
- Follow all cyber safety guidelines, including those related to responsible internet usage.

By adhering to these responsibilities, students contribute to a secure, functional, and collaborative ICT environment for their school community.

Usernames and Passwords

Each student will be allocated an EdPass account, which includes a unique username and password. This account grants access to essential network resources, including:

- All networked printers.
- The internet via a high-speed, filtered connection.
- An individual school email account.

The allocated password serves to protect the student's storage space and internet access. It is the student's responsibility to ensure their password remains confidential and is not shared with anyone. Sharing passwords is strictly prohibited.

To maintain the security and integrity of the school's network, comprehensive monitoring and logging systems are in place. These procedures are used for systems management and to monitor student activity, particularly internet usage, ensuring responsible use of resources.

Flash Drives and External Devices

Flash drives can introduce viruses to the school's network. Their use is permitted only for transferring school-related files or creating backups and should not be relied on for secure storage.

Key Guidelines:

- All files transferred via flash drives may be scanned for viruses before being opened on the school network.
- The school reserves the right to inspect and, if necessary, confiscate flash drives that pose a risk to network security.

Although the school regularly updates its virus protection software, it cannot guarantee that the network is entirely virus-free. Students may be required to show the contents of their flash drives to Management if requested.

Internet Usage

The internet is an essential tool in our teaching and learning programs. It is accessible via a high-speed, content-filtered connection on all networked computers throughout the school. Students may use the internet during class only for research and completing assignments, as directed by their subject teacher.

Guidelines for Internet Use:

- Internet activity is logged and monitored, with all access linked to the user's unique ID. Protecting personal passwords is critical, as misuse under someone else's ID may have serious consequences.
- Only the approved school email client may be used to send and receive emails.
- Students must not visit sites containing violent, racist, sexist, pornographic, offensive, or illegal material.
- Download volumes are monitored to ensure bandwidth is used solely for school-related purposes.
- Accessing chat lines or downloading programs is only permitted with explicit teacher direction.
- Accessing or playing games or music online is not permitted unless explicitly directed by a teacher.

Inappropriate Use:
Misuse of the internet is treated as a serious offence and can result in significant consequences. For example, sending messages under someone else's name may constitute a criminal act.

Artificial Intelligence (AI)

As part of our commitment to enhancing student learning, our school uses artificial intelligence (AI) tools, including ChatGPT, to support educational activities. These tools assist students with tasks such as research, problem-solving, and learning complex concepts.

Parents/carers are advised of the following:

- ChatGPT stores and processes user interactions, and its use aligns with the platform's terms of service, which can be accessed at *https://openai.com/policies/terms-of-use*
- The platform is used strictly for educational purposes and under teacher supervision.
- The school monitors student use to ensure compliance with ICT and behaviour policies.

Parents/Carers are required to sign the relevant agreement form, confirming their acknowledgment of the terms outlined above, before students are permitted to access the ChatGPT platform.

Cyber Safety Agreement Details

Core Values and Practices

Lucindale Area School is committed to fostering a safe and respectful online learning environment for all students. This commitment is guided by our core values and a strong cyber-safety culture. Rigorous measures have been implemented, including the introduction of Cyber Safety Use Agreements, which must be signed by both students and parents/caregivers before students can access school ICT resources.

The school provides child protection education, such as the *Keeping Safe* curriculum, to help students remain safe when engaging with new technologies. ICT resources—including the school's computer network, internet facilities, and other ICT devices—are available for educational purposes only, whether used on or off school grounds.

This Agreement outlines obligations, responsibilities, and the consequences of breaches to ensure that all community members uphold a safe school environment. Students must return their signed User Agreement to gain access to ICT equipment.

Cyber Bullying, E-Crimes, and Inappropriate Material

These definitions and examples are provided to help students understand the boundaries of acceptable bahaviour:

- **Cyber-Safety:** The safe use of internet and ICT equipment/devices, including mobile phones.
- **Cyber Bullying:** The use of internet or mobile technologies (e.g., email, chat rooms, instant messaging, webpages, or SMS) to bully, threaten, or harass others.
- **ICT Equipment/Devices:** Includes desktops, laptops, tablets, USB drives, cameras, mobile phones, audio/video players, and similar devices.
- **Inappropriate Material:** Content involving violence, cruelty, or other unsuitable material harmful to children or inconsistent with the school's values.
- **E-Crime:** Any use of ICT resources to commit, target, or store evidence of unlawful activity.

Parent/Caregiver Responsibilities

Parents and caregivers play an active role in reinforcing cyber-safety by:

- Discussing the importance of following school cyber-safety guidelines with their child.
- Emphasising the need for responsible and ethical online behaviour at all times.
- Ensuring supervision and safe internet practices at home, including the use of filtering software where applicable.
- Contacting the principal or school representatives for queries or concerns regarding cyber-safety.

By signing the relevant agreement, parents/carers confirm their understanding of the outlined terms and their commitment to supporting the school's cyber-safety initiatives.

Strategies for Safe Practice:

To help maintain a secure and respectful digital environment, students must adhere to the following guidelines:

1. Only use school ICT equipment for approved educational purposes.
2. Log in to the school network using their personal username and keep their password private.
3. Access the internet, email, and ICT tools only with teacher permission and under supervision.
4. Avoid inappropriate online activity, such as seeking violent, offensive, or harmful materials, circumventing security systems, or engaging in cyber bullying.
5. Report inappropriate content or incidents that upset or harm them to a teacher immediately.
6. Obtain written permission from both the school and home before bringing personal devices to school or connecting them to school ICT systems.
7. Follow copyright laws when downloading or copying files (e.g., music, videos, or programs) and always seek permission from the teacher or content owner.
8. Respect the school's ICT resources, including avoiding attempts to hack systems, disrupt operations, or damage equipment.

Sanctions of Misuse

ICT Misuse Consequences

Lucindale Area School views the misuse of ICT resources seriously, as it affects the safety, integrity, and functionality of the school's systems.

Students who engage in inappropriate use can expect the following consequences:

- Access to the school's ICT equipment and network may be restricted or revoked.
- Students may be held financially responsible for damages, requiring payment for the repair or replacement of equipment.
- External storage devices containing unauthorised or inappropriate files may be confiscated.
- Unauthorised programs, files, or content found installed on school devices will be removed.
- Personal electronic devices misused for illegal or inappropriate activities (e.g., cyber bullying) will be confiscated and handed to the police for further investigation.
- In cases of serious breaches, including illegal online activity (e-crimes), incidents will be reported to the police.
- Damage caused to laptops hired on a daily or term basis due to misuse will result in repair or replacement costs being billed to the family.

These measures are enforced to protect the learning environment and uphold the school's cyber-safety principles.

Disciplinary Actions

In addition to the technical consequences outlined in the ICT Misuse Consequences, students who misuse the school's ICT resources will face disciplinary measures in alignment with Lucindale Area School's Behaviour Management Policy.

These actions may include:

- Notification to parents or caregivers, including discussions to address the misuse and facilitate corrective actions.
- Implementation of appropriate disciplinary measures, including detentions or suspension of privileges, depending on the nature and severity of the misuse.
- Escalation to school leadership for further review and intervention.
- Exclusion from ICT-related lessons, activities, or programs, where necessary.

In cases of repeated or severe breaches, additional actions may be taken, including consultation with parents/caregivers, increased monitoring, and formalised plans to ensure compliance.

Technical Support and Maintenance

Reporting Issues

Students must report any issues with laptops or ICT Systems to the school's ICT department promptly.

Routine Maintenance

Proper maintenance of laptops is crucial to minimise problems and ensure smooth operation.

Students and Parents are reminded of the following:

- The school will periodically require the laptop to perform routine maintenance, upgrades, and system checks. Some tasks will occur automatically when the student is logged onto the school network or during shutdown.
- Maintenance may include re-imaging the laptop in cases of significant operational issues. This process will restore the device to its original configuration, erasing all data on the hard drive. Students are responsible for backing up their data.
- Technical support for school-issued laptops is available only during school hours and applies solely to resolving issues with school equipment. The school does not provide support for home configurations, such as internet or printer setups.

Safety Maintenance Guidelines:

- Allow sufficient ventilation by keeping the area around the laptop clear. Avoid placing the device on your lap to prevent overheating.
- Keep laptops away from food, drinks, sunlight, sand, and water. Always store the laptop in a padded sleeve or bag for protection.
- Report any hardware or software issues immediately to the Front Office to ensure prompt assistance

Data Backup

Laptop users are responsible for ensuring their data is securely backed up using the recommended methods. The use of Office 365 OneDrive is strongly encouraged, as it allows files to be saved and accessed from any device by logging into office.com using the student's email address.

Best Practices for Data Backup:

- Back up files at the end of each day to minimise data loss.
- Note that if a laptop is sent to ICT Support for repairs, the hard drive may be wiped, and programs reinstalled, which will erase all personal data stored locally on the device.

Students are solely responsible for safeguarding their data. Files should be saved appropriately to OneDrive or backed up to an external drive to ensure they remain accessible at all times.

The school does not provide technical support for issues related to home use, such as internet or printer setup and configuration.

Miscellaneous Policy Notes

Security Practices

Students are responsible for ensuring the security and proper use of their laptops and other ICT equipment by following these guidelines:

- Always secure laptops in a locked classroom or designated storage area when not in use.
- Laptops must be stored in a padded sleeve or protective bag to prevent physical damage during transport.
- Avoid leaving laptops unattended in public spaces or unsecured locations.
- Never leave laptops or other ICT devices in extreme conditions, such as direct sunlight, near water, or in environments prone to sand or dust exposure.
- Take laptops home each night to charge, as they should not be left at school overnight.

By adhering to these security practices, students contribute to protecting school equipment and maintaining a safe and reliable ICT environment.

Virus Protection

The school ensures that anti-virus and monitoring software are installed on all laptops during the initial imaging process. Scheduled updates to the anti-virus software may occur periodically to maintain protection against new threats.

As laptops are permitted for personal use and can connect to the internet at home, students must take proactive measures to safeguard their devices from virus attacks.

Viruses can infiltrate devices through:

- Removable media such as CDs, DVDs, and USB memory sticks.
- Emails and files attached to email correspondence.
- Internet browsing, including accessing unsecured websites, FTP programs, and chat rooms.

By following proper virus protection practices, students contribute to maintaining the security and reliability of their devices and the school's IT environment.

Private Devices

Lucindale Area School provides students with access to a secure and monitored internet system via the school's network. Strict filtering rules block unsafe or inappropriate content, including sites, images, downloads, and data.

Restrictions:

- Personal devices such as mobile phones or dongles must not be used for hot spotting on school grounds, as this bypasses the security measures enforced by the school and Department.

Internet Usage at Home:

Students may set up their laptops to access the internet through their home Internet Service Provider. However, any inappropriate downloads made at home will be detected when the laptop reconnects to the school's network.

Reference and Support

Useful Online Resources

The following websites offer valuable information and tools to support safe and responsible use of ICT and the internet:

http://www.cybersafetysolutions.com.au

http://www.acma.gov.au

http://www.kidshelp.com.au

http://www.bullyingnoway.gov.au

Contacts

For assistance with ICT-related issues or further information, please contact the school's administration office, and they will direct you to our ICT staff.