Policy and Procedure Register updates

Summary of changes to:

Use of ICT services, facilities and devices procedure

1. Reason for new/updated policy or procedure *(select all that apply)*		
☒ Change of policy/procedure requirements	☒ Audit/review recommendation	
☐ Change to legislation/delegations	☒ Due for review	☐ Other

The Use of ICT services, facilities and devices procedure (the procedure) replaces the Use of ICT systems procedure, which was due for review in November 2018. Revision was needed to reflect recommendations from the Crime and Corruption Commission (CCC)'s Operation Impala *Report on misuse of confidential information in the Queensland Public Sector – February 2020* and changes to policies under the Queensland Government's Enterprise Architecture.

Updates to the procedure aim to provide a more comprehensive process for the use and management of ICT services, facilities and devices for students and employees. More recent technologies have been added to the definitions for services, facilities and devices to ensure the procedure continues to provide relevant guidance for employee and student use of ICT.

The procedure is supported by the Use of ICT services, facilities and devices guideline (the guideline) which has been updated with minor changes to include the Managed print services and Backup procedure sections from the outgoing procedure.

2. Summary of changes

The procedure has been updated to align to PPR requirements.

The Managed print services, Closed circuit television and other video surveillance, Network utilities, Email signature block and Metadata schemes sections have been removed. This information is now adequately covered by other procedures in the PPR, OnePortal, the guideline or is no longer mandatory.

The titles of some sections have been updated to clarify the purpose for the audience, for example the 'Internet' section has been renamed to 'Departmental websites' and the 'Identity (ID) and access management' section is now the 'Managing access to ICT services, facilities and devices' section. Sections have been expanded to provide more process information for employees to follow, and sub-sections have been added to help distinguish different steps in the process.

3. Impacts to roles and responsibilities

Does the new/updated content change staff roles/responsibilities *in any way*?	☒ Yes	☐ No

If yes, select the type of change: *(select all that apply)*

☒ Revised responsibilities	☒ New/additional responsibilities	☒ Removed responsibilities

Position title	**Summary of change**	**Page#**
Employees	Responsibilities related to managed print services are now in the guideline.	2

	Responsibilities have been streamlined.	
Business System Owners	Renamed from 'Owners and/or custodians when implementing or updating an ICT business system' and removed from Responsibilities section, now mentioned throughout the procedure. Definition of Business System Owner provided. Responsibilities within the procedure have been reduced due to section removals.	3, 11
Principals	Responsibilities now clearly defined for monitoring school websites and social media for the purposes of school groups and activities.	2
Managers, principals, directors or above	Responsibilities section for all roles are more clearly defined.	2
Director, ICT Infrastructure Services, Digital Innovation Division	Removal of direct responsibility for managed print services. Responsibility now lies with principals, directors or above and is now in the guideline.	2

4. Communication and support for implementation

Changes to the procedure have been communicated with the relevant internal stakeholders. Consultation was conducted across the department and included input from subject matter experts and relevant directors within the Digital Innovation Division (DID).

Department wide communication via OnePortal and ConnectEd will be developed in consultation with the DID communication team.

For further assistance, please contact:

- Policy/procedure contact:

  Governance, Risk and Compliance Unit
  Email: ictpolicy@qed.qld.gov.au

Procedure

Use of ICT services, facilities and devices procedure

Version: 2.0 | **Version effective**: 13/07/2026

Audience

Department-wide

Purpose

This procedure outlines the responsibilities and processes for the acceptable access and use of the Department of Education's (department) information and communication technology (ICT) services, facilities and devices. It provides guidance to schools on regulating employee and student use of ICT.

Overview

The department allows students and employees to access ICT services, facilities and devices for educational purposes and departmental business. Employees are committed to the acceptable use of departmental ICT and use it to undertake various activities directly or indirectly to perform their responsibilities. Principals monitor student use and access to these ICT services, facilities and devices.

Acceptable use of ICT includes professional development, business or school use and limited personal use. Inappropriate use of ICT by students or employees is reported and the relevant parties are notified.

The access and use of departmental ICT services, facilities and devices requires responsible management practices, education, training and employee accountability.

Use of departmentally provided ICT on privately-owned devices (such as accessing government email or Wi-Fi services) must comply with this procedure. However, the use of privately-owned devices more broadly is out of scope.

This procedure is supported by the:

- Advice for state schools on acceptable use of ICT services, facilities and devices
- Information and communication technology (ICT) policy
- Non-departmental ICT service providers procedure
- Use of ICT facilities, services and devices guideline (DoE employees only)

- Use of mobile devices procedure.

Responsibilities

Employees

- use ICT services, facilities and devices appropriately
- report inappropriate use of ICT to supervisor, manager, principal, director or above
- report suspicious or unsolicited ‘spam’ or ‘phishing’ emails
- acquire, install and use software in accordance with department procedures and software licences
- ensure department websites follow accessibility and usability requirements.

Managers, principals, directors or above

- assess and approve requests for user accounts to the department's ICT business systems limiting access where appropriate
- continually manage employee access to the department's ICT business systems and risks posed by unauthorised access to information
- resolve or progress incidents of employees’ inappropriate use of ICT
- manage the updates, licences, and fees to software that has been purchased in their business unit or school
- oversee the maintenance of a software asset register within the OneSchool Asset Register or SAP asset register
- where appropriate, review, remove and restrict access to websites or applications hosting inappropriate content which involves employees, students or implicates a school or the department
- retire, replace and coordinate the uninstallation of software
- undertake an annual review of software compliance in their business unit or school.

Principals

- oversee student access to the department's applications and ICT business systems
- assess and deactivate student accounts to the department's ICT business systems
- follow the school’s emergency response process if inappropriate web content uploaded to a website or application is a threat to employees, students or a community member
- monitor school websites and social media created for the purposes of school groups and activities.

Process

Managing access to ICT services, facilities and devices

The department controls and restricts access to its ICT business systems to prevent breaches and misuse. The following section outlines how the department manages ICT access for students and employees.

Employee access requests to ICT business systems

Employees may require access to several different ICT business systems to fulfil their role. Access to some systems will be granted when employees start with the department. To request access to ICT business systems:

- Employees use the iRegister system (DoE employees only) to request access to the department's ICT business systems and applications including the corporate VPN, EduWorkspace and some Microsoft 365 applications.
- Managers, principals, directors or above review access requests and must consider:
  - if an employee needs system access to fulfil their role (refer to Identity default access entitlements (DoE employees only) (KBA0019201) in Services Catalogue Online (SCO))
  - restricting access to information classified as PROTECTED following the Information security procedure.

For further information about requesting and managing access to departmental ICT business systems refer to the iRegister (DoE employees only) OnePortal page.

Other forms of access to ICT business systems

- If non-departmental users are given temporary access to ICT business systems, managers, principals, directors or above must either:
  - put in place controls so non-departmental users can only access the information they need to fulfil their role
  - have an appropriate departmental employee with system access supervise the non-departmental user.
- For schools, principals can approve the use of generic accounts from within iRegister considering the risks, benefits, cost, ongoing management and alternative options. See the Create a new generic account (DoE employees only) (KBA0018946) for more information.

Ongoing management of ICT business systems

- Managers, principals, directors or above who control access to an application or ICT business system must:
  - make sure user access application forms include a privacy collection statement that indicates how personal information is collected, will be used and protected. See the Privacy collection notices (DoE employees only) OnePortal page for information on privacy statements
  - educate employees and students annually (or when system updates require) about the password and security requirements of ICT business systems:
    - for password requirements see the Network Password Requirements help article (DoE employees only) (KBA0020064)
    - for security requirements see the Cyber security (DoE employees only) OnePortal page
  - immediately notify Business System Owners when an employee's access should be deactivated for unacceptable use of ICT business systems. Refer to the Use of ICT services, facilities and devices guideline (DoE employees only) for more details
  - disable or modify employee access to the relevant system if they:

        - resign
        - are seconded
        - take a prolonged period of leave
        - are dismissed or suspended
    - ensure ICT business systems are approved, managed and established following departmental processes and ICT standards
    - review employee access at least once every quarter making sure access levels are appropriate. If access needs to be updated and cannot be updated through iRegister, log a General enquiry request (DoE employees only) in SCO
    - continue to protect the identities of employees and enrolled students who have become subject to legal orders so only authorised employees (for example, manager, principal or delegate) have access
    - encourage employees to make sure their details are kept up to date where work identification and location details are provided within a directory.

Managing and deactivating a student's account

- Principals are responsible for overseeing student access to the department's applications and ICT business systems and:
    - must use the Managed Internet Service (MIS) (DoE employees only) to temporarily deactivate a student's access such as email and internet access if they are suspended, excluded, or due to their inappropriate use
    - must use OneSchool to manage changes to students' enrolment status
    - are responsible for the actions which occur on all active accounts, including those which should be deactivated.
- Principals may deactivate a student's account due to inappropriate use or for the duration of vacation periods by following the article Suspend/disable a student's identity (DoE employees only) (KBA0014976). They must use a risk assessment approach which considers:
    - the impact on the student's education or training outcomes
    - the likelihood the system or network will be used inappropriately
    - if the student has a history of inappropriate use
    - whether the student's need for access to complete course requirements outweighs the protection of the system or network.
- To disable a student account immediately, the principal should contact the school's technician or contact the IT Service Centre.

School ICT policy

- Principals must ensure a policy outlining the acceptable and legal use of departmental ICT is developed for their school. This can be added to the Student Code of Conduct information regarding the use of mobile phones and other devices, or can take the form of a procedure, policy, statement or guideline. The policy should also include information for students and parent/carers about student personal mobile

device access. Further advice and a template are available within the Advice for state schools on acceptable use of ICT services, facilities, and devices.

- Principals must ensure the school's acceptable and legal use of ICT policy is understood and acknowledged by school students and parent/carers at least annually, either on the date of enrolment or through communication with parent/carers at the start of each school year.

Employee use of ICT services, facilities and devices

Employees access and use of departmental ICT is appropriate and aligns with the department's ICT policy, Code of Conduct and Standard of Practice. While personal use of departmental ICT is permitted, it must be limited, infrequent, undertaken when not working (such as lunch breaks or outside of scheduled work hours) where possible, and done without impacting other employees or the operation of government. However, personal use of departmentally owned mobile devices within a State Delivered Kindergarten (SDK) is restricted. Further information for SDKs is provided within the Safe use of digital technologies and online environments policy (DoE employees only).

Refer to the Use of ICT services, facilities and devices guideline (DoE employees only) for full details on acceptable and unacceptable use.

Acceptable use

- Employees' access to intranet, internet and network usage is monitored and email messages sent or received by anyone using the department's ICT business systems may be inspected to:
  - identify inappropriate use
  - protect system security
  - maintain system performance
  - protect the rights and property of the department
  - determine compliance with state, Commonwealth and departmental policy.

Limited personal use

- Employees' appropriate use of the department's ICT includes limited personal use (excluding the personal use of departmentally owned mobile devices within an SDK). Personal use includes checking personal social media, calling a family member on a desk phone, or completing study or personal banking. Employees must ensure personal use:
  - is infrequent
  - is done during off-duty hours, like lunch breaks or before or after work
  - does not disrupt government operations or incur additional costs to the department
  - does not disrupt their own or anyone else's work
  - does not extend to personal, financial or commercial gain.

Reporting inappropriate use

- Employees must report inappropriate use of ICT services, facilities or devices to their supervisor, manager, principal, director or above. Examples of inappropriate use include:

  - the access, creation, transmission or storage of pornographic, racist, violent, or any other unacceptable content
  - to collect, access, use or disclose personal information for an unauthorised purpose
  - use of gambling websites or applications
  - installation or use of restricted applications such as TikTok and DeepSeek
  - using their privately-owned email accounts for departmental business
  - use of software in breach of the licensing conditions
  - disabling or interfering with the operation of antivirus software
  - attempting to bypass cyber security controls
  - excessive personal use
  - sharing passwords to ICT business systems or applications they can access.
- Once notified the supervisor, manager, principal, director or above must:
  - resolve the incident locally where possible
  - if the incident cannot be resolved locally, submit an Information security incident (DoE employees only) SCO form or contact the following (as appropriate):
    - for technology issues contact IT Service Centre on 1800 680 445 or SCO (DoE employees only)
    - for a privacy breach to the Privacy team using the Report a privacy breach (DoE employees only) SCO form in accordance with the Privacy data breach and complaints procedure
    - for violations of the Queensland Government's Code of Conduct for the Queensland Public Service contact Integrity and Employee Relations.

If the department reasonably suspects an employee's misuse of the network may be misconduct, corruption, or a criminal offence under section 426(4A) of the *Education (General Provisions) Act 2006* (Qld), it will report the case to the police.

Report suspicious emails

- Employees may receive suspicious or unsolicited 'spam' or 'phishing' emails which:
  - ask for sensitive information, such as bank details
  - encourage people to open a malicious attachment
  - link to a fake website which asks for sensitive information or downloads malicious content without a user knowing.
- If employees receive a suspicious email, they must report it and avoid clicking on any links they contain.
- Employees report suspected 'spam' or 'phishing' emails to the Cyber Security Operations team by using the 'Report' button located in the Outlook toolbar or by forwarding the email as an attachment to operational.security@qed.qld.gov.au.

Reporting inappropriate web content accessed or uploaded by students or employees

Supervisors, teachers, managers, principals, directors or their delegate must follow this process to remove and report inappropriate content uploaded to any websites or applications (whether departmentally-owned or not), particularly if employees and students are involved or the school or department is implicated in some way. This includes content uploaded on privately-owned or departmental devices and situations where the content identifies the person as an employee (or student, parent/carer etc.). Any accidental access by a student or employee to inappropriate sites or where access to a site leads to inappropriate content must be reported to their relevant supervisor, teacher, manager, principals, directors or their delegate for review.

Supervisors, teachers, managers, principals, directors or their delegate review the web content (where accessible) and determine the actions to be taken.

- If the website or application is blocked by the department's network:
  - contact the IT Services Centre by phone (1800 680 445) to discuss available options
  - contact the Cybersafety and Reputation Management Team (07 3034 5035), or
  - log a Cybersafety enquiry (DoE employees only) SCO form for further investigation.
- If the content poses a threat to school employees, students or any community member the principal follows the school's emergency response process and reports the incident to the Regional Director.
  - School, regional or central office employees who need to contact local law enforcement must refer to the Disclosing personal information to law enforcement agencies procedure and complete a Disclosure of personal information to a law enforcement agency (LEA) form.
- Supervisors, teachers, managers, principals, directors or their delegate must facilitate the removal of the content and:
  - where possible, direct the student or employee responsible for uploading the content to remove it from the website or application
  - coordinate the content's removal with the website/application owner or service provider:
    - content hosted on social media can be directly reported on the hosting page
    - content hosted on other websites will need to be removed directly by their owners. The owner's details can normally be found on the bottom of the web page
  - if further assistance is required:
    - refer to the Remove harmful online content (DoE employees only) SCO form
    - contact the Cybersafety and reputation management team (DoE employees only) or their IT Customer Manager (DoE employees only).
- Supervisors, teachers, managers, principals, directors or their delegate must minimise access to the offensive content:
  - schools can contact their Managed Internet Service administrator (DoE employees only) to immediately 'block' the website or application at the school level
  - regional and central office can use the Unblock or block a website (Corporate) (DoE employees only) SCO form to request a departmental 'block'.

- If personal information has been uploaded supervisors, teachers, managers, principals, directors or their delegate must contact the Privacy Team and refer to the Privacy data breach and complaints procedure.
- Supervisors, teachers, managers, principals, directors or their delegate should report any incident that has grounds for discipline and meets the threshold for misconduct (as defined in the Public Sector Act 2022 (Qld)) to the Integrity and Employee Relations unit.
    - schools can report the incident via iRefer (DoE employees only)
    - regional and central offices can report the incident by:
        - sending an email to intake@qld.gov.au
        - calling 1800 468 253
        - via mail to: Manager, Intake and Assessment, Department of Education, PO Box 15033, City East, Qld, 4002.

For school specific ICT responsible use requirements refer to the Advice for state schools on acceptable use of ICT services, facilities and devices.

Software applications and software licences management

All software, including free and open-source software (OSS), must be purchased, installed or implemented, used and managed in compliance with this procedure and any licensing terms and conditions that may restrict where and how it is used.

Using unauthorised or unlicensed software, or violating software licensing terms of use, can present reputational, legal and cyber security risks to the department and its employees. To minimise these risks, follow the steps below.

Purchasing and installing licensed software

All employees must:

- not install, or attempt to install, unlicensed or unauthorised software on any departmental ICT devices
- acquire all online services in line with the Non-departmental ICT service providers procedure
- seek approval from a manager, principal, director and above to purchase or obtain software licenses
    - specific instructions and forms for requesting some software, such as Adobe Creative Cloud, are available through the Software and business systems (DoE employees only) in SCO
- install software on departmental ICT devices using the appropriate software request form on SCO (DoE employees only). If no dedicated form exists, use the General software (DoE employees only) SCO form.

Teachers, managers, principals, directors and above must:

- coordinate purchases in compliance with the Purchasing and procurement procedure and ICT asset management procedure
- ensure that software licences are procured under the name of 'The State of Queensland acting through the Department of Education'.

Using and managing licensed software

All employees must:

- understand and follow their obligations under the licensing terms and direct any software licence enquiries such as compliance and eligibility using the General enquiry (DoE employees only) SCO form
- ensure free software for privately-owned devices such as Microsoft Office 365 (DoE employees only) and Adobe Creative Cloud (DoE employees only) complies with its conditions of use including uninstalling the software when leaving the department or deleting the software when their ICT device is sold or disposed of
- notify a supervisor, manager or above about unlicensed or unauthorised software (including any privately-owned) on departmental ICT devices that needs to be uninstalled
- ensure privately-owned mobile devices connected to the department's network have appropriate licenses for the software being used.

Teachers, managers, principals, directors and above must:

- manage licensed software in accordance with the ICT asset management procedure
- take full responsibility for the management of directly purchased software, including updates, licensing, fees and compliance to its terms and conditions of use
- maintain a Software asset register (DoE employees only) to monitor, record and manage software use (including the storage of original media and licence documentation, but excluding licences distributed as part of the department's managed operating environment (MOE)). To register software assets:
  - schools use the OneSchool Asset Register (DoE employees only)
  - regional and central offices use SAP asset register (DoE employees only)
- coordinate an annual review of software compliance in their business unit or school (this excludes licences distributed under the MOE)
- coordinate the uninstallation of software identified as unlicensed, unauthorised, inappropriate or deemed as an unsupported application using a General software (DoE employees only) SCO form
- ensure school managed bring your own device programs comply with software licensing conditions for privately-owned devices.

Considerations for open-source software (OSS)

All employees must:

- not use OSS applications where whole of government applications have been mandated for use, such as SAP financial management
- undertake a business impact assessment which includes advice from Legal Services and the appropriate copyright licence before contributing to or releasing any departmental OSS.

Teachers, managers, principals, directors and above must:

- acquire any OSS in accordance with the Queensland Government's Open source software guideline and seek Software licensing team approval (DoE employees only) (KBA0018403) before installing it on departmental devices

- ensure that use, modification and distribution of OSS software adheres to the OSS licence conditions.

Departmental websites

All departmental websites must be hosted on web hosting services authorised by the Assistant Director-General (ADG), Digital Products and Assurance. This includes websites created to support school and classroom activities.

- Employees with permission to edit content on school or corporate websites must ensure the website follows accessibility and usability requirements consistent with Queensland Government standards and branding guidelines. This includes:
  - regularly reviewing and updating content so it remains current and accurate
  - appropriate metadata and records management processes
  - following the Queensland Government's Digital service policy and the Web Content Accessibility Guidelines
  - providing contact information, privacy notices, provisions for customer feedback and information requests, disclaimer notices, and the appropriate Creative Commons licence.
- Principals are responsible for their school's web publishing. School based employees can request access to edit content on their school website or request website support via the Websites for Schools support (DoE employees only) SCO form. The relevant principal must approve these requests within SCO where required.
- Principals are also responsible for monitoring websites and social media created for the purposes of school groups and activities, such as Parents and Citizens' associations and sporting groups, to ensure users maintain appropriate privacy and respectful interactions. For further guidance refer to the Social media for school and departmental promotion procedure or the Queensland Government's Principles for the use of social media networks and emerging technologies.
- Employees in corporate business units can log a request to publish, update or remove content they are responsible for on departmental websites via a Web work request (DoE employees only) SCO form. The approvals required depend on the nature and urgency of the request, for more information refer to the Web work request (DoE employees only) OnePortal page.
- Employees can request an investigation into whether the Web Content Accessibility Guidelines or web content quality assurance reviews apply to their situation via the Quality assurance requirements assessment (DoE employees only) SCO form.
- Web and Digital Production (WDP) (DoE employees only) unit can provide advice on web content publishing and web-based solutions for both corporate business units and state schools. For more information refer to the OnePortal Website publishing page (DoE employees only) or schools can contact their IT Customer Manager (DoE employees only).

Use of domain names

Employees must use the correct domain name (e.g. qld.gov.edu.au) when creating a website or application. All new domain name requests (including sub domain names or domains five levels deep in the hierarchy) must be reviewed and approved by WDP.

Requesting a new domain name

- Employees seeking a new domain name must contact WDP via domainname.admin@qed.qld.gov.au. WDP will assess this request to:
  - ensure the correct domain name is used, or that an exemption has been provided (see below)
  - determine whether associated costs apply (schools are not required to pay for their primary domain name but additional domain names may incur a cost)
  - ensure the approved process has been followed.
- WDP will respond to the requestor and, if approved by the Director, WDP, will manage the submission with the domain name provider.
- Employees must promote domain names in accordance with the Queensland Government's Domain name registration and management standard to ensure advertising and sales collateral is not ordered until the domain name has been secured.
- The Director, WDP is the nominated delegate as the single point of contact within the department for registrations with the Queensland Government domain provider.

Exemptions

- Employees can seek exemptions from the department's domain name requirements by submitting a business case to the ADG, Digital Products and Assurance for approval. The submission must:
  - be in the form of a general briefing note
  - outline why an exemption is needed.
- The ADG, Digital Products and Assurance will assess the submission and approve or deny the request.

Decommissioning a domain name

- If employees want to de-register or decommission a domain name, related website or application they can seek advice from WDP. WDP will assist the school, regional office or business unit with the decommission process in accordance with the Information asset and recordkeeping procedure.

Backing-up information stored on ICT devices and business systems

- Employees must not store the only copy of important information on storage media that is not regularly backed up such as local hard drives (internal such as C: and D: drives or external) of computers or removeable media. Network drives and departmentally authorised recordkeeping systems are regularly backed up by the department.
- Business System Owners who locally manage ICT business systems and applications will need to follow backup rules and set controls as outlined in the Use of ICT services, facilities and devices guideline (DoE employees only).

Definitions

Term	Definition
Authorised recordkeeping systems	An ICT business system designed to capture, manage and provide access to records through time, that is intended to preserve the context, authenticity and integrity of the records. Authorisation is provided by a principal, an executive director or above, ensuring compliance with recordkeeping requirements such as Public Records Act 2023 (Qld) and Queensland Government's Records governance policy. Examples of approved recordkeeping systems include Content Manager for regional and central offices, the OneSchool (DoE employees only) suite of applications for schools or suitable secure file location on school servers. ICT business systems that do not qualify as an authorised recordkeeping system include email systems (such as Outlook), OneDrive, Teams, QChat. Further information can be found in OnePortal under Records management (DoE employees only).
Business System Owner	An employee who has authority and accountability for an information asset and associated ICT resources and approves the rules by which the asset is managed. Ownership is often delegated to the operational Assistant Director-General or Executive Director. Owner may be referred to as information owner, Business System Owner, application owner, or system owner For example, the Director of Enterprise Information Services is the Business System Owner for Content Manager and the Principal of a school is the Business System Owner for IDAttend.
Employee	Any permanent, temporary, seconded, casual or contracted staff member, contractors and consultants or other person who provides services on a paid basis to the department that are required to comply with the department's policies and procedures. Within schools this includes principals, deputy principals, heads of department, heads of curriculums, guidance officers, teachers and other school staff. Volunteers depending on the engagement may not be considered employees but should have regard for this procedure.
ICT business system	Information technology systems or applications designed to automate and support the undertaking of a specific business process or processes. They may create, receive, manage and maintain business information relating to business processes. They include ICT services, facilities and devices.
ICT devices	Electronic or digital devices/equipment designed for a particular communication and/or function, including but not limited to computers, mobile devices, television sets, interactive panels and boards, gaming/esports (DoE employees only) consoles and equipment, augmented or virtual reality equipment, AV/media

Term	Definition
	streaming and storage devices, and digital or analogue records such as DVD and video, photocopiers/printers and other imaging equipment.
ICT facilities	An electronic capability designed for a particular communication and/or function, which includes but is not limited to electronic networks, online environment, internet, extranet, email, instant messaging, artificial intelligence (AI) including generative AI, webmail, fee-based web services and social media.
ICT services	Telecommunications services that carry voice and/or data and includes applications, hosting, storage, and cloud-based services etc.
IT Customer Manager	IT Customer Managers (DoE employees only) are part of Customer Engagement within Digital Innovation Division. Their responsibilities include communicating and directing policies, plans and services within schools, supporting schools with strategic planning, gathering requirements for future services and products within schools, capturing feedback and managing expectations of schools.
Mobile device	A portable digital computing or communications device with information storage capability that can be used from a non-fixed location. Mobile devices include, but are not limited to, mobile and smart phones, smart watches and wearable devices, laptops, notebooks, tablets, personal digital assistants (PDA), eBook readers, game devices, voice recording devices, cameras, USB drives, flash drives, DVDs/CDs or hard disks, and other electronic storage media or hand-held devices that provide retention and mobility of data.
Online services	Online (or digital) services are websites, web applications and mobile applications that are delivered over the internet or require an internet connection. They are used to meet a range of needs for education, collaboration and connectivity for students and employees. Examples of online services include interactive learning sites and games, online collaboration and communication tools, web-based publishing and design tools, learning management systems, file storage and collaboration services. They can be free or paid subscriptions and may or may not be provided by the department.
Open-source software	Open-source software is software that can be freely accessed, used, changed, and shared (in modified or unmodified form) by anyone. Open-source software is made by many people and distributed under licenses that comply with the Open Source Definition.
Personal information	Information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion: • whether the information or opinion is true or not, and

Term	Definition
	• whether the information or opinion is recorded in a material form or not.
Privately-owned mobile device	A mobile device owned wholly by the individual or employee and not by the department, or whereby the mobile device is being paid for by the individual under an arrangement with the department where at the end of the arrangement the individual will privately own the device. Also known as a personal electronic device. It also includes bring your own device (BYOx) initiative.

Legislation

- Criminal Code Act 1899 (Qld)
- Education (General Provisions) Act 2006 (Qld)
- Information Privacy Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Public Sector Act 2022 (Qld)

Delegations/Authorisations

- Nil

Policies and procedures in this group

- Information and communication technology (ICT) policy
- Non-departmental ICT service providers procedure
- Use of mobile devices procedure
- ICT asset management procedure

Supporting information for this procedure

- Advice for state schools on acceptable use of ICT services, facilities, and devices

Other resources

Department of Education

- CCTV use in schools procedure
- Code of conduct for the Queensland public service
- Cyber security (DoE employees only)
- Disclosing personal information to law enforcement agencies procedure
- Equipment management for business units procedure

- Equipment management for schools procedure
- ICT standards (DoE employees only)
- iRegister (DoE employees only)
- IT Customer Manager (DoE employees only)
- Managed Internet Service (DoE employees only)
- OneSchool Asset Register (DoE employees only)
- Orange Card Holders (DoE employees only)
- Reporting spam or phishing emails (DoE employees only)
- Safe use of digital technologies and online environments policy (DoE employees only)
- SAP asset register (DoE employees only)
- Services Catalogue Online (SCO) (DoE employees only)
- Social media for school and departmental promotion procedure
- Use of ICT facilities, services and devices guideline (DoE employees only)

Whole of government

- Digital services policy
- Domain names policy
- Domain name registration and management standard
- Open source software guideline
- Principles for the use of social media networks and emerging technologies
- Use of internet and email policy

External

- World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines (WCAG)

Contact

For further information on ICT policies and procedures contact:
Governance Risk and Compliance unit, Digital Innovation Division
Email: ictpolicy@qed.qld.gov.au

Review date

13/07/2029

Superseded versions

Previous seven years shown. Minor version updates not included.

Creative Commons licence

Advice for state schools on acceptable use of ICT services, facilities and devices

This document supports the Use of ICT services, facilities and devices procedure and Use of mobile devices procedure by providing advice to state schools on the acceptable use of information and communication technology (ICT) services, facilities and access by departmental or personally-owned devices.

This advice provides the following information:

- ICT and the curriculum – an overview of the importance of ICT within schools
- Personal mobile device access – implementation of controls for school employees' personal mobile devices and students' personal mobile devices
- Student access to the department's ICT services, facilities and devices – controls that need to be considered when allowing students to access the Department of Education's (DoE) (department's) network
- School-specific ICT responsible use procedure – a template to assist schools in creating an ICT responsible use procedure
- Community access to state school ICT facilities and devices – ICT considerations when managing community activities within a school environments.

ICT and the curriculum

Students use ICT as an integral part of their learning and to equip them to live and work successfully in the digital world. In the Prep to Year 10 Australian Curriculum in all learning areas, students develop capability in using ICT for tasks associated with information access and management, information creation and presentation, problem-solving, decision-making, communication, creative expression and empirical reasoning. This includes conducting research, creating multimedia information products, analysing data, designing solutions to problems, controlling processes and devices, and supporting computation while working independently and in collaboration with others.

Students develop knowledge, skills and dispositions around ICT and its use, and the ability to transfer these across environments and applications. They learn to use ICT with confidence, care and consideration, understanding its possibilities, limitations and impact on individuals, groups and communities.

Personal mobile device access

The department is aware that limited personally-owned mobile device access is essential for the effective running of schools. The department reserves the right to restrict access of personally-owned mobile devices to ensure the integrity of the network and a safe working and learning environment for all network users. These mobile devices include but are not limited to mobile phones, laptops, tablet devices, voice recording devices (whether or not integrated with a mobile phone or MP4 player), handheld gaming devices (e.g. Nintendo Switch, Sega Genesis), smart watches, SD cards or USBs.

If in doubt when implementing technical requirements around the management of personally-owned mobile devices and access to the department's ICT facilities and devices, **advice can be sought from** the IT Service Centre on 1800 680 445. **Policy advice** can be sought directly from Manager, Information and Governance Management on 3034 5093. Additionally, information is available via the Services Catalogue Online (DoE employees only).

School employees personal mobile device access

Principals are to ensure that school employees follow the requirements under the Use of mobile devices procedure.

Student personal mobile device access

Widespread access to the network by student personally-owned mobile devices could compromise the integrity of the department's ICT network. Principals, however, can determine that for educational purposes a student can have access to the department's ICT network. This connection is provided only if the personally-owned mobile device meets the department's security requirements at a minimum by enabling the locking of the personal mobile device, such as a passcode/password, face recognition and/or fingerprint, and where possible installing and managing their own anti-virus software.

Schools wanting students to connect to the department's ICT network are required to develop procedures to ensure that such provisions are assessed against the department's security requirements (where necessary undertaking a risk assessment) and that students and their parents/guardians are provided with the necessary education and assistance to be able to meet these departmental requirements.

The procedures must include:

- providing advice to all students and their parents/guardians on appropriate security requirements (see iSecurity (DoE employees only) website for details)
- advising teachers/supervisors as soon as any breach of security is suspected
- the right to restrict/remove student access to the intranet, internet, email or other network facilities if they do not adhere to the school's network usage and access policy, guideline or statement
- ensuring that students are aware of occupational health and safety issues when using computers and other learning devices.

Schools that are implementing or have implemented the Bring Your Own 'x' (BYOx) (DoE employees only) process also need to ensure steps have been taken to provide a safe and effective learning environment for students while meeting the department's security requirements. This includes advising parents/guardians that the devices provided allow access to their home and other out of school internet services and that such services may not include any internet filtering.

Student access to the department's ICT services, facilities and devices

The department's *Digital Strategy 2024-2028* supports the investment in new foundations for contemporary learning, with near-seamless access to information and digital technologies at any time, any place and on any device. Essential tools for providing these innovative educational programs include the intranet, internet, email and network services (such as printers, display units and interactive whiteboards) that are available through the department's ICT network. These technologies are vital for the contemporary educational program provided in schools.

At all times students, while using these ICT services, facilities and devices, will be required to act in line with the requirements of the Student Code of Conduct and any specific rules of their school. In addition, students and their parents should:

- understand the responsibility and behaviour requirements (as outlined by the school) that come with accessing the department's ICT services and network facilities
- ensure they have the skills to report and discontinue access to harmful information if presented via the internet or email
- be aware that:
  - access to ICT services, facilities and devices provides valuable learning experiences for students and supports the school's teaching and learning programs
  - ICT services, facilities and devices should be used appropriately as outlined in the Student Code of Conduct
  - the school is not responsible for safeguarding information saved/stored by students on departmentally-owned student computers or mobile devices
  - schools may remotely access departmentally-owned student computers or mobile devices for management purposes

  - students who use a school's ICT services, facilities and devices in a manner that is not appropriate may be subject to disciplinary action by the school, which could include restricting network access
  - illegal, dangerous or offensive information may be accessed or accidentally displayed despite internal departmental controls to manage content on the internet
  - teachers will always exercise their duty of care, but avoiding or reducing access to harmful information also requires responsible use by the student
- any inappropriate images/footage posted by individuals on website/s is managed according to the Online incident management guideline for school leaders (DoE employees only).

School-specific ICT responsible use procedure

The Use of ICT services, facilities and devices procedure provides direction to school principals around formulating a school procedure on access to the department's/school's ICT services, facilities and devices for parents and/or students to understand and acknowledge. This may take the form of a procedure, policy, statement or guideline and may require consultation with the school community. Acknowledging through signing seeks to support an understanding of what is lawful, ethical and safe behaviour when using or accessing the department's network and facilities by students and their parents. Principals may seek sign-off either on enrolment of students or alternatively at the start of each school year. Students should be reminded of their responsibilities at the beginning of each school year.

The following dot points are to assist schools to formulate their own procedure. Further guidance on drafting this section can be sought from the Use of ICT facilities and devices guideline.

Purpose statement

- Information and communication technology (ICT), including access to and use of the internet and email, are essential tools for schools in the provision of innovative educational programs.
- Schools are constantly exploring new and innovative ways to incorporate safe and secure ICT use into the educational program.
- School students, only with the approval of the principal, may be permitted limited connection of personally-owned mobile devices to the department's network, where this benefits the student's educational program.

Authorisation and controls

The principal reserves the right to restrict student access to the school's ICT services, facilities and devices if access and usage requirements are not met or are breached. However restricted access will not disrupt the provision of the student's educational program. For example, a student with restricted school network access may be allocated a stand-alone computer to continue their educational program activities.

The Department of Education monitors access to and use of its network. For example, email and internet monitoring occurs to identify inappropriate use, protect system security and maintain system performance in determining compliance with state and departmental policy.

The department may conduct security audits and scans, and restrict or deny access to the department's network by any personal mobile device if there is any suspicion that the integrity of the network might be at risk.

Responsibilities for using the school's ICT facilities and devices

- Students are expected to demonstrate safe, lawful and ethical behaviour when using the school's ICT network as outlined in the Student Code of Conduct.
- Students are to be aware of occupational health and safety issues when using computers and other learning devices.
- Parents/guardians are also responsible for ensuring students understand the school's ICT access and usage requirements, including the acceptable and unacceptable behaviour requirements.
- Parents/guardians are responsible for appropriate internet use by students outside the school environment when using a school-owned or school-provided mobile device.
- The school will educate students (DoE employees only) regarding cyber bullying, safe internet and email practices, and health and safety regarding the physical use of ICT devices. Students have a responsibility to adopt these safe practices.
- Use of the school's ICT network is secured with a user name and password. The password must be difficult enough so that it cannot be guessed by other users and is to be kept private by the student and not divulged to other individuals (e.g. a student should not share their username and password with fellow students).

- Students cannot use another student's or staff member's username or password to access the school network. This includes not browsing or accessing another person's files, home or local drive, email or accessing unauthorised network drives or systems. Additionally, students should not divulge personal information (e.g. name, parent's name, address, phone numbers), via the internet or email, to unknown entities or for reasons other than to fulfil the educational program requirements of the school.
- Students need to understand that copying software, information, graphics or other data files may violate copyright laws without warning and be subject to prosecution from enforcement agencies.

Responsibilities for using a personal mobile device on the department's network

- Prior to using any personally-owned mobile device, students must seek approval from the school principal to ensure it reflects the department's security requirements.
- Students are responsible for the security, integrity, insurance and maintenance of their personal mobile devices and their private network accounts.
- Where possible, appropriate anti-virus software has been installed and is being managed.
- Students must follow any advice provided on best security requirements e.g. password protection (see iSecurity (DoE employees only) website for details).
- Students and parents are to employ caution with the use of personal mobile devices particularly as these devices can store significant numbers of files some of which may be unacceptable at school e.g. games and 'exe' files. An 'exe' file ends with the extension '.exe' otherwise known as an executable file. These files can install undesirable, inappropriate or malicious software or programs.
- Any inappropriate material or unlicensed software must be removed from personal mobile devices before bringing the devices to school and such material is not to be shared with other students.
- Unacceptable use will lead to the mobile device being confiscated by school employees, with its collection/return to occur at the end of the school day where the mobile device is not required for further investigation.

Acceptable/appropriate use/behaviour by a student

It is acceptable for students while at school to:

- use mobile devices for:
  - assigned class work and assignments set by teachers
  - developing appropriate literacy, communication and information skills
  - authoring text, artwork, audio and visual material for publication on the intranet or internet for educational purposes as supervised and approved by the school
  - conducting general research for school activities and projects
  - communicating or collaborating with other students, teachers, their parents or experts in relation to school work
  - accessing online references such as dictionaries, encyclopaedias, etc.
  - researching and learning through the department's eLearning environment
- be courteous, considerate and respectful of others when using a mobile device
- switch off and place out of sight the mobile device during classes, when these devices are not being used in a teacher-directed activity to enhance learning
- use their personal mobile device for private use before or after school, or during recess and lunch breaks, in accordance with Student Code of Conduct
- seek teacher's approval where they wish to use a mobile device under special circumstances.

Unacceptable/inappropriate use/behaviour by a student

It is unacceptable for students while at school to:

- use a mobile device in an unlawful manner
- download, distribute or publish offensive messages or pictures
- use obscene, inflammatory, racist, discriminatory or derogatory language
- use language and/or threats of violence that may amount to bullying and/or harassment, or stalking

- insult, harass or attack others or use obscene or abusive language
- deliberately waste printing and internet resources
- damage computers, printers or network equipment
- commit plagiarism or violate copyright laws
- ignore teacher directions regarding the use of social media, online email and internet chat
- send chain letters or spam email (junk mail)
- share their own or others' personal information and/or images which could result in risk to themselves or another person's safety
- knowingly download viruses or any other programs capable of breaching the department's network security
- use in-phone cameras inappropriately, such as in change rooms or toilets
- invade someone's privacy by recording personal conversations or daily activities and/or the further distribution (e.g. forwarding, texting, uploading, Bluetooth use etc.) of such material
- use the mobile phone (including those with Bluetooth functionality) to cheat during exams or assessments
- take into or use mobile devices at exams or during class assessment unless expressly permitted by school employees.

Sign-off

The sign-off process for school students and their parents/guardians should occur on enrolment and annually. The following is a suggested format, with the signature block to be placed at the end of the agreement.

Please note: Children from Prep to Year 3 inclusively are exempt from signing the student section below.

Student:

I understand that the school's information and communication technology (ICT) services, facilities and devices provide me with access to a range of essential learning tools, including access to the internet. I understand that the internet can connect me to useful information around the world.

While I have access to the school's ICT services, facilities and devices: I will use it only for educational purposes; I will not undertake or look for anything that is illegal, dangerous or offensive; and I will not reveal my password or allow anyone else to use my school account.

Specifically in relation to internet usage, should any offensive information appear on my screen I will close the window and immediately inform my teacher quietly, or tell my parents/guardians if I am at home.

If I receive any inappropriate emails at school I will tell my teacher. If I receive any at home I will tell my parents/guardians.

When using email or the internet I will not:

- reveal names, home addresses or phone numbers – mine or that of any other person
- use the school's ICT service, facilities and devices (including the internet) to annoy or offend anyone else.

I understand that my online behaviours are capable of impacting on the good order and management of the school whether I am using the school's ICT services, facilities and devices inside or outside of school hours.

I understand that if the school decides I have broken the rules for using its ICT services, facilities and devices, appropriate action may be taken as per the school's Student Code of Conduct, which may include loss of access to the network (including the internet) for a period of time.

I have read and understood this procedure/policy/statement/guideline and the Student Code of Conduct.

I agree to abide by the above rules/the procedure/policy/statement/guideline.

_____ (Student's name)

_____ (Student's signature) _____ (Date)

Parent or Guardian:

I understand that the school provides my child with access to the school's information and communication technology (ICT) services, facilities and devices (including the internet) for valuable learning experiences. In regards to internet access, I understand that this will give my child access to information from around the world; that the school cannot control what is available online; and that a small part of that information can be illegal, dangerous or offensive.

I accept that, while teachers will always exercise their duty of care, protection against exposure to harmful information should depend upon responsible use by my child. Additionally, I will ensure that my child understands and adheres to the school's appropriate behaviour requirements and will not engage in inappropriate use of the school's ICT services, facilities and devices. Furthermore I will advise the school if any inappropriate material is received by my child that may have come from the school or from other students.

I understand that the school is not responsible for safeguarding information stored by my child on a departmentally-owned student computer or mobile device.

I understand that the school may remotely access the departmentally-owned student computer or mobile device for management purposes.

I understand that the school does not accept liability for any loss or damage suffered to personal mobile devices as a result of using the department's services, facilities and devices. Further, no liability will be accepted by the school in the event of loss, theft or damage to any mobile device unless it can be established that the loss, theft or damage resulted from the school's/department's negligence.

I believe _____ (name of student) understands this responsibility, and I hereby give my permission for him/her to access and use the school's ICT services, facilities and devices (including the internet) under the school rules. I understand where inappropriate online behaviours negatively affect the good order and management of the school, the school may commence disciplinary actions in line with this user agreement or the Student Code of Conduct. This may include loss of access and usage of the school's ICT services, facilities and devices for some time.

I have read and understood this procedure/policy/statement/guideline and the Student Code of Conduct.

I agree to abide by the above rules / the procedure/policy/statement/guideline.

_____(Parent/Guardian's name)

_____ (Parent/Guardian's signature) _____ (Date)

The Department of Education through its Information privacy breach and privacy complaints procedure is collecting your personal information in accordance with the *Education (General Provisions) Act 2006* (Qld) in order to ensure:

- appropriate usage of the school network
- appropriate usage of personal mobile devices within the school network.

The information will only be accessed by authorised school employees to ensure compliance with its Information privacy breach and privacy complaints procedure. Personal information collected on this form may also be disclosed to third parties where authorised or required by law. Your information will be stored securely. If you wish to access or correct any of the personal information on this form or discuss how it has been dealt with, please contact your child's school. If you have a concern or complaint about the way your personal information has been collected, used, stored or disclosed, please also contact your child's school.

Note: The Australian Mobile Telecommunications Association has published materials which may be of use to schools.

Community access to state school ICT facilities and devices

This section provides guidance for schools and their communities undertaking commercial or cost neutral community activities at the school or other educational facility, which require access to departmental ICT resources. This advice should be used in conjunction with Community use of state school facilities procedure.

The Department of Education encourages schools to provide their communities with access to government funded information and communication technologies (ICT) resources, where such access does not interfere with the normal operation of the school. By providing access to the school's ICT resources, the department, through its schools, is building partnerships that will support the continuing/lifelong learning needs of communities, and improve their ability to participate in future economic, social and educational opportunities.

Educational service delivery is the primary reason for providing ICT in schools. Access to school ICT will be granted only to community organisations that agree to adhere to the policies, procedures, practices and values of the department, and are of good standing. Access is formalised through written agreement between the school and the user or group, and, will be undertaken only if:

- the school has the capacity to extend the use of their ICT resources to community members
- there is a genuine community need for the types of services to be provided under the activity
- the activity does not impact negatively on the school's core business and responsibilities
- the activity does not contravene the *Competition and Consumer Act 2010* (Cwlth) and/or other relevant legislation, and
- the activity complies with contractual and/or licensing agreements held by the department.

This section provides guidance when:

- assessing the initial set-up of the community's access to ICT program and the on-going operation of such a program
- extending their ICT resources for community use.

It does not cover remote access and hand held ICT devices or elements related to schools operating as Registered Training Organisations.

Responsibilities

Principals:

- assess the need and school's capability prior to agreement for the conduct of a community program where access to government funded schools' ICT facilities is requested
- are accountable for:
  - preparation and administration of required documentation
  - management of assets, physical and environmental security and safety issues
  - management of access to ICT equipment and network/internet security
- regularly monitor the community access program to determine impacts on the schools and future continuity.

Regional Technology Managers:

- provide advice to principals when assessing the need and school's capability prior to establishing a community access agreement.

Executive Director, Legal and Administrative Law Branch:

- advise on the development and implementation of legal contracts to formalise agreements for community access to ICT.

Director, Education Workforce Relations:

- advise on appropriate allocation of staff member's involvement in community access to school ICT, particularly with respect to support outside working hours or industrial agreements.

Regional Facilities Manager:

- advise schools on the appropriate use of school facilities, including community access to ICT, in consultation with regional technology managers
- assist with the licensing of premises, including licensing cost calculation.

ICT Service Support:

- assist in establishing on-going ICT operations within schools, including terms of existing ICT licensing arrangements for provision of community access to ICT.

Assistant Director-General, Information and Technologies:

- approves this procedure and any subsequent reviews, amendments, related documents or associated departmental guidelines developed.

Process

Steps to be taken by Principals and/or their delegate:

Preparation and administration of required documentation

- follow the Community use of state school facilities procedure and prepare a hire agreement
- if activity is being managed by the School's Parent & Citizen's Association, ensure they have:
  - liaised with the Queensland Council of Parents and Citizens Association (QCPCA) to discuss issues such as insurance requirements and completion of the activity declaration form
  - a current insurance policy that extends to volunteers involved with these activities
- approve community access to ICT for the school, ensuring the formal hire agreement, is prepared and signed and appropriate rules for the use of the school's ICT are established, adhered to and maintained by all parties
- arrange for participants to sign a hire agreement
- ensure all volunteers sign the School Volunteers Register and sign a Volunteer Agreement
- conduct Criminal History Checks and Working with Children Checks where required for employees and volunteers in accordance with Working With Children Check - Blue Cards procedure.

Management of assets, physical and environmental security and safety issues

- consider the security issues associated with community access to ICT resources and other equipment and ensure appropriate safeguards are put in place to protect these assets (refer to School security procedure)
- ensure that everyone involved in the community access activity is:
  - familiar with use of the school's security system and relevant security procedures
  - aware of their Workplace Health and Safety responsibilities
  - instructed in the use of the school's emergency procedures
  - covered through WorkCover or Public Liability Insurance
- make additional safety arrangements for community access activities conducted at night, for example:
  - adequate lighting to enable staff and community members to enter and exit the school in safety
  - participants are accompanied when walking to their vehicles or leaving school grounds
  - provision of a telephone to allow community members to arrange transport
  - inform P&C members of their need to comply with the confidentiality provisions of the *Education (General Provisions) Act 2006* (Qld)

  - take appropriate steps to protect the physical/overall security and privacy of students and to ensure that inappropriate contact between participants and any students that may be on school grounds after hours is avoided (refer to the department's Student protection procedure)
- ensure that:
  - at least one individual responsible for leading emergency procedures is present whenever the community access activity is being conducted
  - an attendance roll is maintained
  - a telephone or intercom is available to allow staff and community members to communicate if an emergency arises
  - a first aid kit is available as described in Managing first aid in the workplace procedure
- ensure collection, storage and transfer of all monies collected are conducted in accordance with school accounting manual (DoE employees only) and/or the P&C Accounting Manual
- if the school enters into an agreement with another organisation, e.g. the P&C, to jointly provide a community access activity for which external funding has been received, ensure that the monies are not used against the intent of the funding organisation. For example, the P&C might receive a grant from a foundation to run Internet Safety Awareness courses for parents. The intent of the original grant is for such classes and should not be used for another purpose
- determine and agree to future ownership of any assets which may be purchased for the community access program.

Management of access to ICT equipment and network/internet security

- ensure adherence to Use of ICT services, facilities and devices procedure
- ensure all contractual and/or licensing agreements are adhered to, and that providing community access to school ICT does not contravene any ICT provider's licence arrangements
- establish processes to ensure that:
  - any information (physical and electronic) that identifies individual children is removed from the area in which the community access activity is to be held
  - traces of any inappropriate information that community members may have accessed on school computers are removed
  - individuals should be given an individual account registered in their own name, where access to the Managed Internet Service is provided on an on-going basis
- negotiate agreed level of service with technical support staff in accordance with relevant industrial instruments, if technical support is necessary. This may include negotiating on-call arrangements or extended hours of work
- ensure that community members do not have access to areas of the network, in accordance with the Use of ICT services, facilities and devices procedure containing information that could be used to identify:
  - individual students and student records
  - staff personnel records
  - financial information
  - other sensitive information. This may be achieved by password protection, firewalls or establishing a separate isolated drive/Local Area Network

- ensure, in accordance with the Information security procedure that:
  - the latest version of antivirus software is installed on all computers and that virus definition files are up-to-date introduction of viruses is limited by scanning all files and information contained on portable media and storage devices prior to it being used
  - close supervision of participants occurs so that viruses / spyware are not introduced
  - a virus scan is run on new disks and files
- ensure that participants:
  - access the school internet responsibly and in accordance with intent of this document
  - do not corrupt, damage or alter the settings, restrictions or content of the school's computers, either deliberately or inadvertently
  - do not disable or interfere with the operation of antivirus software installed on computers
  - do not introduce viruses or malicious code into the school's systems
  - do not create, knowingly access, download, distribute, store or display any form of offensive, defamatory, discriminatory, malicious or pornographic material
- establish a process to limit the amount of information downloaded by participants, as the network usage may significantly increase as a result of community use.

Last updated: 13 May 2020. Please email ICT policy on any questions or suggested changes required to this advice.