

JUNE 2025

Information and Communications Technology Web Filtering Policy

Table of Contents

Version 1.2 – 4/06/2025

1	Purpose	3
2	Policy Statement.....	3
3	Requirements	3
3.1	All Users	3
3.2	School and College Learners	3
3.3	Libraries, Online Access Centres and Adult Education	4
3.4	Employees	4
3.5	Blocked Categories.....	4
4	Related policies	5
5	Related procedures.....	5
6	Supporting information/tools	5
7	Definitions.....	6
8	Legislation	7

1 Purpose

This policy outlines the Department for Education, Children and Young People's (the department) implementation and requirements for web filtering. Web filtering is technology that prevents users from viewing certain content or websites.

This policy applies to all people who are users of department or Government Information Communication Technology (ICT) resources, including employees, contractors, volunteers, learners, service providers, service users and guests. It also applies to Users who use non-department equipment (including personal devices, such as mobile phones, tablets, laptops, and computers) to access department and Government ICT resources and infrastructure including Wi-Fi.

2 Policy Statement

The department provides Users with access to online information, software, and content via the Internet. Web filtering technologies prevent access from a computer to types of information, software, and content. The department uses filtering technologies to prevent the downloading of software that is potentially malicious, disruptive or that can damage the network or degrade its performance. Web filtering technologies may also restrict access to information and content which is considered inappropriate or illegal based on its subject matter, for example, depictions of violence, pornography, and child sexual abuse material.

The department is committed to providing access to online resources in a safe and productive environment. The department requires all users to use ICT resources appropriately. The department has a responsibility to ensure that usage is consistent with this policy and complies with all relevant legislative requirements, including that Tasmanian State Service employees undertake their duties in accordance with the [State Service Principles](#) and [Code of Conduct](#).

3 Requirements

3.1 All Users

Users must not attempt to bypass web filtering access for themselves or to expose other persons to inappropriate or illegal content. Any concerns that users are attempting to access inappropriate or illegal content, such as child abuse material, will be dealt with in accordance with staff implementing departmental procedures. Illegal activity will also be reported to the Police.

3.2 School and College Learners

Schools have a duty of care to ensure the safety of their learners. This involves providing a safe physical and emotional environment for learners. The use of the internet can generally be considered a foreseeable risk of harm or injury to learners, which schools have a duty of care to take steps to prevent. Schools are required to utilise the department-provided Networking Tasmania web filtering service and are not to allow unfiltered access by learners to the internet.

Web filtering alone is not a web safety solution for schools. Schools are also required to implement ICT Acceptable Use Agreements for learners, ensure appropriate supervision of learners using the internet, and educate learners to participate safely in a global information environment.

3.3 Libraries, Online Access Centres and Adult Education

The State Library of Tasmania and Libraries Tasmania utilise the department-provided Networking Tasmania web filtering service to filter access to the internet to help protect clients from exposure to inappropriate material, and to ensure that such material is not displayed in a public place. Filtering also protects the network from security risks posed by malicious software. Clients are also required to abide by the [ICT Conditions of Use Policy](#). Where a library or online access centre is co-located with a school, filtering is applied at the same level as the school.

Learner access to the internet as part of Adult Education classes is provided for purposes relating to their course of study. Adult Education sites are filtered by the filtering arrangements of the course location.

3.4 Employees

Use of the internet by employees is filtered by the department-provided Networking Tasmania web filtering service. Use of the internet by employees is governed by the departmental [ICT Conditions of Use Policy](#).

3.5 Blocked Categories

The web filtering service uses categorisation to group and block similar websites. The department applies different policies based on the cohorts of employees, learners and clients. Some schools block other categories in addition to the base block categories, e.g. social networking.

CATEGORY BLOCKED	EMPLOYEES	LEARNERS	CLIENTS
Adult	X	X	X
Alcohol		X	
Cannabis	X	X	X
Cheating and Plagiarism	X	X	X
Dating	X	X	X
Dynamic and Residential	X	X	X
Extreme	X	X	X
Filter Avoidance	X	X	X
Gambling		X	
Hacking	X	X	X

CATEGORY BLOCKED	EMPLOYEES	LEARNERS	CLIENTS
Hate Speech	X	X	X
Illegal Activities	X	X	X
Illegal Downloads	X	X	X
Illegal Drugs	X	X	X
Lingerie and Swimsuits		X	
Non-sexual Nudity	X	X	X
Parked Domains	X	X	X
Peer File Transfer	X	X	X
Pornography	X	X	X
Terrorism and Violent Extremism	X	X	X
Tobacco		X	
Weapons	X	X	X

4 Related policies

- [Cybersecurity Policy](#) (staff only)
- [Conduct and Behaviour Policy](#)
- [Information and Communications Technology Conditions of Use Policy](#)
- [Personal Information Protection Policy](#)
- [Social Media Policy](#)
- [Student Behaviour Management Policy](#)
- [Tasmanian Government Cybersecurity Policy](#)

5 Related procedures

- [Duty of Care for Students on Departmental Educational Sites Procedure](#) (staff only)
- [Mandatory Reporting Procedure](#)
- [Respectful Visitors and Volunteer Behaviour Procedure](#)
- [Student Behaviour Management Procedure](#)

6 Supporting information/tools

- [Conduct and Behaviour Standards](#)

- [Cyber Safety Resources](#)
- [ICT Acceptable Use - Information for Parents](#) (staff only)
- [ICT user Agreement - Primary School Students - K – 3](#) (staff only)
- [ICT user Agreement - Primary School Students - 4 – 6](#) (staff only)
- [ICT user Agreement - Responsible Use Letter to Parents for Primary Students](#) (staff only)
- [ICT user Agreement - Secondary School Students](#) (staff only)
- [ICT User Agreement - Use of Mobile Telephone Resources Guidelines for Employees](#) (staff only)
- [Online Child Sexual Abuse Material: Response Flowchart for DoE Staff](#) (staff only)
- [Responding to incidents, disclosures, or suspicions of harmful sexual behaviour Flowchart for Principal/Site Leader/Delegate](#) (staff only)
- [Safe. Secure. Supported. Our Safeguarding Framework](#)
- [Social Media Toolkit](#) (staff only)
- [Step by Step Guidance for Concerns, Information and Incidents of Child Abuse](#) (staff only)

7 Definitions

Child abuse material

Child abuse material includes any material that depicts or describes a child, or a representation of a child, who is or appears to be under the age of 18, and who is or appears to be in a sexual pose or sexual activity, or that shows or describes the person's sexual organs or breasts as a dominant characteristic. This definition includes material that depicts or describes a child, or a representation of a child, as a victim of torture, cruelty or physical abuse.

Information and Communications Technology (ICT) resources

Technological tools, devices and resources used to communicate, create, disseminate, store, and manage information. Examples include but are not limited to computers/laptops, mobile devices, telephones, computer applications/systems, network services and equipment, the internet, email and messaging services, broadcasting technologies (radio and television), audio/video equipment, storage media and devices.

Intellectual property

The legal rights associated with the product of people's imagination and creativity. Intellectual property rights can be dealt with like any other form of property (such as land and goods); i.e. they can be bought, sold, and licensed. Types of intellectual property include copyrights, patents, trademarks, and trade secrets.

Malicious software

Software intentionally designed to cause damage to a computer, server, client, or computer network. Malicious software is also referred to as malware.

Networking Tasmania

A collection of service agreements/arrangements between the Tasmanian Government and Telstra for the provision of data and telecommunications services to government agencies.

Online

Online means controlled by or connected to a computer.

Online child sexual exploitation

Online child sexual exploitation occurs when an individual (adult or another child or young person) or group uses technology or the internet to facilitate the sexual abuse of a child, including the production and sharing of child abuse material online.

Unauthorised access

Unauthorised access is accessing information or resources without permission. Examples include gaining access to a website, system or equipment using someone else's credentials (or other methods). Unauthorised access may also occur if a user attempts to access an area of a system or data repository they should not be accessing.

User

A user is any person (adult, child, or young person) who accesses and uses department ICT resources, including employees, contractors, volunteers, learners, service providers, service users, and guests.

Web filtering

Technology that prevents users from viewing certain content or websites.

8 Legislation

Includes, but is not limited to the following legislation and employment directions:

- [Anti-Discrimination Act 1998](#)
- [Spam Act 2003](#)
- [State Service Act 2000](#)
- [State Service Regulations 2021](#)
- [Employment Direction No. 5 – Procedures for the Investigation and Determination of whether an employee has breached the Code of Conduct](#)
- [Employment Direction No. 12 – Internet and Email Use by State Service Officers and Employees](#)

Authorised by: Trevor Hill, Director Information Technology Services

Contact: Information Technology Services, Service and Help Centre.

Request assistance online at help.education.tas.gov.au

For urgent requests telephone (03) 6232 7799.

Last significant review: 7 September 2023

Review due: 7 September 2028

This document replaces: Version 1.1

Key search words: ITS, web filtering, use, users, ICT resources, monitoring access and use