<table>
<thead>
<tr>
<th></th>
<th>Purpose</th>
<th>Policy Statement</th>
<th>Related policies</th>
<th>Related procedures</th>
<th>Supporting information/tools</th>
<th>Definitions</th>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Purpose</td>
<td>Policy Statement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Principles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Related policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Related procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Supporting information/tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Legislation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1 Purpose

The purpose of this policy is to define and communicate what is deemed as acceptable use by all users granted access to Information and Communications Technology (ICT) resources provided and/or owned by the Department for Education, Children and Young People (the department) and/or the Tasmanian Government (Government).

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

2 Policy Statement

The department provides users with ICT resources to support work and learning related tasks. The appropriate use of ICT materially improves the capacity of workers and learners to undertake day-to-day activities, and aims to eliminate the risk of online abuse, including online child sexual exploitation and online child sexual abuse (including grooming).

The department expects all users to use ICT resources appropriately and has a responsibility to ensure that usage is consistent with this policy and complies with all relevant legislative requirements. This includes Tasmanian State Service employees undertaking their duties in accordance with the State Service Principles and Code of Conduct.

2.1 Principles

The department and Government ICT resources, and the services accessible through these resources, are provided to help users undertake their work or learning and fulfil their roles and responsibilities.

Use of these resources must be appropriate to each user’s role and not jeopardise the integrity, security, or service levels of the department, nor harm the reputation of the Government or the department, its users, workplaces, clients, or other stakeholders.

All access to and use of ICT resources must be able to withstand public scrutiny and/or disclosure.

2.1.1 Employee responsibilities and accountabilities

Employees and other adult users:

- Are responsible and accountable for their work-related and private actions that may impact the department or the Government.
- Must ensure their behaviour and conduct always complies with:
  - Legislation, including but not limited to national and state privacy and copyright laws and the State Service Act 2000.
  - Department policies, procedures and guidance that defines behaviours and activities that are unacceptable and/or inappropriate, including the Professional Standards for Staff Policy and Guidelines and the Social Media Toolkit.
  - General expectations of acceptable and appropriate behaviour, including taking care not to interact in any way that could be perceived to be harassing, discriminatory, victimising or otherwise unacceptable or inappropriate. This also includes behaviour that could lead to learners, employees or other users being exposed to image-based abuse, sexting, cyberbullying.
online child sexual exploitation, online sexual abuse (including grooming), stalking, or exposure to unreliable information or illicit materials.

Failure to comply with these principles and the requirements of legislation and this policy may lead to disciplinary and/or other action, as appropriate.

Actions associated with adherence to and implementation of this policy must be appropriately authorised in accordance with the department’s Delegations and Administrative Authorities.

The following arrangements must be followed to support the department’s commitment to ensuring the appropriate use of ICT resources.

2.1.2 Online child sexual abuse and online child sexual exploitation

Department and Government ICT resources must not be used to perpetrate any kind of online child sexual exploitation or child sexual abuse, including grooming.

Engaging in online child sexual exploitation or child sexual abuse is a criminal offence. users who engage in the sexual exploitation or abuse of a child online may be prosecuted. State Service employees who engage in these activities may also be subject to disciplinary action under the State Service Act 2000.

Employees are ‘prescribed persons’ with Mandatory Reporting Procedure obligations under the Children, Young People and Their Families Act 1997. Any employee who has a concern, belief, suspicion or knowledge that a child or young person is being exposed to, or is a victim of, online child sexual exploitation or abuse must report that information to the Strong Families Safe Kids Advice and Referral Line (ARL) by telephone on 1800 000 123. Please refer to the following documents for more information about reporting requirements:

- Mandatory Reporting Procedure
- Advice for Staff - Responding to incidents, disclosures and suspicions of child sexual abuse
- Responding to incidents, disclosures or suspicions of harmful sexual behaviour Flowchart for Principal/Site Leader/Delegate.

2.1.3 Reasonable personal use

The department accepts the occasional personal use of ICT resources by users, providing that use:

- Does not adversely impact the productivity or work performance of any individual.
- Does not deliver a cost to the department (directly or indirectly)
- Is consistent with community expectations and general standards of accepted behaviour for workers.
- Does not disrupt ICT systems or department business.
- Does not introduce security risk to the department or Government.
- Does not harm the department or the Government’s reputation.
- Does not involve inappropriate use of ICT resources (refer below).

2.1.4 Inappropriate use of ICT resources

Users must not access or use ICT resources to:

- Commit crimes or engage in any unlawful activity.
- Affect the integrity and good reputation of the State Service.
• Harass (including to sexually harass), discriminate, abuse, threaten, insult or breach orders (such as Family Violence Orders).
• Transmit, store, view, copy or display obscene or pornographic imagery, including child abuse material or other objectionable or illegal material (unless required and permitted to do so as part of their duties).
• Perpetrate image-based abuse.
• Conduct unauthorised profit-making or commercial activities.
• Conduct unauthorised political activity.
• Distribute unsolicited advertising material from organisations having no connection with the department or involvement in its activities in line with the Australian Spam Act 2003.
• Use department ICT resources (including email addresses or department-issued mobile phones or phone numbers) to subscribe to, or regularly consume, online services for personal purposes.
• Gain, or attempt to gain, unauthorised access to any computer service or resource (internal or external to the Department).
• Access client or customer information without a Legitimate work-related need.
• Knowingly permit use of, or access to, ICT resources by non-authorised individuals. For example, a family member using a work mobile phone.
• Use ICT resources in ways that are likely to corrupt, damage or destroy data, software, or hardware, either belonging to the department or to anyone else, whether inside or outside the department or Government network (unless specifically authorised as part of their duties).
• Save or install licensed department software on private ICT resources without formal approval from the Director IT Services (ITS).
• Save or install personal software or any other form of software on department-provided or Government-provided devices or ICT resources without formal approval by the Director ITS, or by exception if ITS provides advice that this action is permitted within the department’s licence agreement.
• Make or store any unauthorised reproductions of material protected by copyright or use audio-visual items in which copyright subsists. All software must be used in accordance with their licence agreements.
• Attempt to repair, interfere with, or add any devices (whether hardware or components) to any ICT resource, unless authorised and competent to do so. This includes deliberately damaging or tampering with physical ICT equipment, cabling, or other configurations, or knowingly permitting such damage by others.
• Use another person’s login or password or allow others to use yours.

2.1.5 Waiver of liability
The department restricts access to some material available via the internet, but does not accept responsibility for any illegal, offensive, indecent, or otherwise harmful material accessed on the internet, nor for any loss, however arising, associated with using or relying on information obtained through its internet service or in relation to the reliability or quality of that service.

2.1.6 Acceptable Use Agreements and guidelines
Acceptable Use Agreements or guidelines may be developed to assist compliance with this policy and provide assurance that different cohorts of users understand their ICT conditions of use obligations under this policy.
It is important to note that the department’s ICT resources are accessed and used by a diverse range of users with different capacities to understand and abide by their specific obligations. Agreements and guidelines should therefore be developed to address the needs and requirements of specific user groups or use cases, as and when appropriate.

2.1.7 Monitoring access and use

User access and usage of ICT resources are subject to continuous monitoring, which includes the department’s right to review the content of emails, social media usage and details of web usage.

Users should be aware that their activity on all ICT systems may be audited.

Monitoring activities are supported by the department’s Cybersecurity Policy, and the Tasmanian Government’s Cybersecurity Policy.

2.1.8 Managing alleged inappropriate use of ICT

Managers are responsible for providing information to users to help them understand their responsibilities and enable appropriate use of ICT resources in accordance with the requirements of this policy.

If a manager becomes aware of potentially unacceptable or inappropriate use of ICT resources by any user, they should discuss the issue directly with the user (if appropriate to do so) to explore any mitigating circumstances and/or provide options for remediating action. Depending on the situation, the manager may be able to manage the user’s behaviour/conduct informally or more formally within the scope of the department’s behaviour or performance management framework.

If a user’s behaviour/conduct constitutes or is likely to constitute a breach of legislation and/or the State Service Code of Conduct, the manager should seek advice from Human Resources and the relevant delegate to support management of the issue. This may require:

- Issuing a request to ITS to initiate relevant investigations into, or monitoring of, the user’s interaction with ICT resources.
- Commencement of a Code of Conduct investigation process.
- Advising the relevant employee that an investigation has commenced.

2.1.9 Recordkeeping and reporting inappropriate use of ICT

Managers must ensure that all discussions about the inappropriate use of ICT resources are documented and recorded in accordance with the department’s Records Management Policy.

All information about the use of department and/or Government ICT resources to perpetrate any kind of online child sexual exploitation or child sexual abuse, including grooming, must be recorded and reported in accordance with Section 2.1.2 of this policy and the Mandatory Reporting Procedure.

Access to information about targeted monitoring/investigations into use of ICT resources by a user will occur in line with usual processes and requirements, including those associated with Code of Conduct investigations.

2.1.10 Delegations

Actions associated with this policy and any associated processes must be appropriately authorised in accordance with the department’s Delegations and Administrative Authorities.
3 Related policies

- **Cybersecurity Policy**
- **Personal Information Protection Policy**
- **Professional Standards for Staff Policy**
- **Social Media Policy**
- **Tasmanian Government Cybersecurity Policy**
- **Web Filtering Policy**

4 Related procedures

- **Duty of Care for Students on Departmental Educational Sites Procedure**
- **Mandatory Reporting Procedure**

5 Supporting information/tools

- **Mandatory Reporting Procedure**
- **Advice for staff - Responding to incidents, disclosures, and suspicions of child sexual abuse**
- **Responding to incidents, disclosures, or suspicions of harmful sexual behaviour Flowchart for Principal/Site Leader/Delegate**
- **Safeguarding Framework**
- **Conduct and Behaviour Standards**
- **ICT Acceptable Use - Information for Parents [KB0021115]**
- **ICT user Agreement - Primary School Students - K – 3 [KB0015348]**
- **ICT user Agreement - Primary School Students - 4 – 6 [KB0021116]**
- **ICT user Agreement - Responsible Use Letter to Parents for Primary Students [KB0015369]**
- **ICT user Agreement - Secondary School Students [KB0015349]**
- **ICT user Agreement - Use of Mobile Telephone Resources Guidelines for Employees [KB0015335]**
- **Online Child Sexual Abuse Material: Response Flowchart for DoE Staff**
- **Professional Standards for Staff Guidelines**
- **Social Media Toolkit**
6 Definitions

Child sexual abuse
Child sexual abuse is any act (including grooming) that exposes a child to, or involves a child in, sexual processes that are beyond their understanding, are contrary to accepted community standards, or are outside what is permitted by law.

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.

Cyberbullying
Bullying that is carried out through the internet or mobile phone technologies, including sending or sharing threatening, intimidating, harassing or humiliating content to or about someone.

Grooming
Grooming means any online or in-person behaviour intended to manipulate and control a child, their family, kin or carers, or other support networks or organisations, with the aim of: gaining access to the child, obtaining the child’s compliance, maintaining the child’s silence, and/or avoiding discovery of sexual abuse; grooming may be difficult to identify and can be done by people already known to the child, including by a child’s family member, kin or carer.

Image-based abuse
Image-based abuse means when intimate, nude or sexual images are shared without the consent of those depicted, or a threat to share the content is made, including images or videos that have been digitally altered, photoshopped or drawn.

Information and communications technology (ICT) resources
Technological tools, devices and resources used to communicate, create, disseminate, store, and manage information. Examples include 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, etc.

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. Also referred to as malware.

Mandatory reporting
The legal requirement to report a reasonable belief of child abuse to the responsible authorities.

Online
Online means controlled by or connected to a computer.
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.

Online grooming

Online grooming is the process of establishing and building a relationship with a child through use of the internet or other technologies to facilitate sexual contact with that child, either physically or online. It may include perpetrators encouraging victims to engage in sexual activity or to send the perpetrator sexually explicit material. It may also lead to perpetrators meeting the victim in person or blackmailing the victim to self-produce explicit materials.

Sexting

Means self-generated digital content/images of a sexual nature taken by a person of themselves and shared with others. Sexting may also be referred to as personal image sharing, sending a ‘selfie’ or a ‘pic’ (note that content depicting a person under the age of 18 can be considered child abuse material and an offence to produce, store or distribute under Australian legislation.

Unauthorised access

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.

7 Legislation

Includes, but is not limited to:

- State Service Act 2000
- State Service Regulations 2021
- Anti-Discrimination Act 1998
- Spam Act 2003
- 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