DEPARTMENT OF EDUCATION, SPORT AND CULTURE

RHEYNN YNSEE, SPOYRT AS CULTOOR

Isle of Man Government

Reiltys Ellan Vannin

Acceptable Use

Policy for DESC Schools

Glossary

Authorised personnel are members of staff from the school, Department or GTS who are authorised to perform systems administration and/or monitoring of the ICT facilities.

Data protection legislation for the purposes of this Policy includes:

- Data Protection Act 2018;
- Data Protection (Application of GDPR) Order 2018;
- Data Protection (Application of LED) Order 2018;
- GDPR and LED Implementation Regulations 2018.

Department means the Department of Education, Sport and Culture, including schools, UCM, Villa Gaiety and Manx Sport & Recreation.

DESC has the same meaning as 'Department' above.

DPO means the Department's Data Protection Officer

GTS means Government Technology Services, an office within the Cabinet Office of the Isle of Man Government.

ICT facilities means all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service that may become available in the future which is provided as part of the school's ICT service.

Learner means any child or young person who is enrolled at a school in the Island.

Materials means files and data created using the school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

Personal use means any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user.

Schools means any primary or secondary school that is a "provided school", as defined by section 2(5)(a) of the Education Act 2001 and listed in Schedule 1, Part 1 of the same Act.

SIRO means the Department's Senior Information Risk Owner.

Users means anyone authorised by the school to use the school's ICT facilities, including governors, staff, learners, volunteers, contractors and visitors.

Contents

Summary

About this policy

Information and communications technology (ICT) is an integral part of the way our schools work, and is a critical resource for pupils, staff, governors, volunteers and visitors.

However, the ICT facilities our schools use could also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT facilities for staff, pupils, parents/carers and governors;
- Establish clear expectations for the way all members of the schools' communities engage with each other online;
- Support the Department's and schools' other policies, particularly those regarding data protection, mobile phone use, behaviour/relationships and safeguarding;
- Prevent disruption that could occur to schools through the misuse, or attempted misuse, of ICT facilities; and
- Support schools in teaching safe and effective internet and ICT use.

Who is this document for?

This policy is for all persons present on the premises of any school maintained by DESC, including the leaders, staff, volunteers, pupils, visitors and the Governing Bodies.

It may also be referenced by parents/carers and the wider public for information.

Key points

This policy covers all users of schools' ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under each school's behaviour/relationship policy, staff code of conduct etc.

Effective date

This document is effective from January 2025. It will be kept under review and updated at least every two years.

Policy

1. Unacceptable Use

1.1. Unacceptable use of school ICT facilities includes, but is not limited to:

- Using school ICT facilities to breach intellectual property rights or copyright
- Using school ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching school or Department policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Online gambling, inappropriate advertising, phishing and/or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams – *please refer to the Department's Nudes and Semi-Nudes Guidance*
- Activity which defames or disparages the Department or one of its schools, or risks bringing the Department or one its schools into disrepute
- Sharing confidential information about the department or one of its schools, its pupils, or other members of the school community
- Connecting any device to a school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on a school's network without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Inserting USB drives
- Installing games and other .exe files
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to a school's ICT facilities
- Causing intentional damage to a school's ICT facilities
- Removing, deleting or disposing of a school's ICT equipment, systems, programmes or information without permission from authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by authorised personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to a school

- Using websites or mechanisms to bypass school filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

AI

1.2. The following uses of AI and generative chatbots are not acceptable:

- During assessments, including internal and external assessments, and coursework; and
- To write homework or class assignments, where AI-generated text or imagery is presented as the learner's own work.

1.3. However, a school's head teacher may use their discretion to grant an exemption for the use of AI and generative chatbots, where it is deemed acceptable. Examples of such circumstances include:

- As a research tool to help learners find out about new topics and ideas; and
- When specifically studying and discussing AI in schoolwork, e.g. in IT lessons or art homework about AI-generated images.

1.4. Where the use of AI is permitted, all AI-generated images and work must be properly attributed.

2. Staff (including governors, volunteers and contractors)

Access to school ICT facilities and materials

2.1. Each school is responsible for coordinating access to its ICT facilities and materials for school staff. This includes, but is not limited to:

- Computers, tablets, mobile phones and other devices; and
- Access permissions for certain programmes or files.

2.2. Staff use of ICT facilities must be in accordance with the Isle of Man Government 'Acceptable Use' staff handbook.

Use of email, the internet and social networking tools

2.3. Staff must not share their personal email address(es) with parents/carers and learners, and must not use their personal email address(es) for work purposes.

Use of personal devices

2.4. Before personal devices can be used to access or store Government information, approval must first be obtained from the Department's SIRO and only GTS-supported solutions may be used, along with any security measures that are provided to you.

2.5. All use of mobile phones and smart devices, whether personal or provided by work, must be in accordance with the Department's Mobile Phone and Smart Devices policy.

Remote access

2.6. When carrying out work outside schools or other Government workplaces, staff must use an approved remote access solution and be aware of their surroundings, to ensure that Government information is secure and not openly visible to others.

School social media accounts

2.7. If a school has any official social media accounts, these must only be managed by staff who have been authorised to do so by the head teacher.

Social media and electronic communications

2.8. All electronic communications and use of social media by staff must be in line with the Isle of Man Government's Electronic Communications and Social Media: Policy, Standards and Guidelines, with consideration for the Guidelines for the Use of Electronic Communications and Social Media.

3. Learners

Access to ICT facilities

3.1. Each school is responsible for determining which ICT facilities are available to learners, including when and for what purposes they are to be used.

Confiscation of personal devices

3.2. Use of personal smart devices by learners is governed by the Department's Mobile Phones and Smart Devices policy.

Unacceptable use of ICT facilities and the internet outside of school

3.3. In line with their behaviour / relationship and other relevant policies, each school will take appropriate actions where a learner engages in the following activities, even if they have not occurred on school premises:

- Breaching the school's and/or Departments policies;
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity;
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate;
- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams;
- Inserting USB drives;
- Installing games and other .exe files;
- Activity that defames or disparages the school, or risks bringing the school into disrepute;
- Sharing confidential information about the school, other learners, or other members of the school community;

- Gaining or attempting to gain access to restricted areas of the Department's or a school's network, or to any password-protected information, without approval from authorised personnel;
- Allowing, encouraging or enabling others to gain, or attempt to gain, unauthorised access to the school's ICT facilities;
- Causing intentional damage to a school's ICT facilities or materials;
- Causing a data breach by accessing, modifying or sharing data to which a user, and/or those they share it with, are not supposed to have access or without authorisation.

4. Parents / Carers

Access to ICT facilities

4.1. Parents/carers do not have access to school ICT facilities.

4.2. However, where parents/carers are working for or with a school in an official capacity, they may be granted an appropriate level of access, or be permitted to use the school's ICT facilities at the head teacher's discretion.

4.3. Where access is granted, the parents/carers must abide by this policy as it applies to staff.

5. Working Securely with ICT Facilities

Access to ICT facilities and materials

5.1. All users of a school's ICT facilities will have clearly defined access rights to school systems, files and devices.

5.2. Users must not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is granted in error, or if something a user should not have access to is shared with, they should alert the Department's DPO immediately, as any high risk data breaches must be reported to ICO within 72 hours. Staff should also contact the IT administrator or GTS to have their permission updated or changed.

5.3. To avoid unauthorised access, users should always log out of systems and lock their devices when they are not in use.

5.4. Systems and devices should always be logged out of and shut down at the end of each working day.

Passwords

5.5. All users of ICT facilities are responsible for the safekeeping of their account details, which includes the setting of secure passwords.

5.6. Passwords must be at least nine characters in length and must contain at least three of the following:

- Numbers
- Upper case letters
- Lower case letters

- Special characters (e.g. ! $ %).

5.7. Passwords that are easy to remember should be difficult for somebody else to guess

5.8. Do not write down or give out your passwords, smartcards or tokens.

5.9. Use passwords for your school and Government accounts that are different from any personal passwords you use.

Data protection

5.10. All personal data must be processed in line with data protection legislation, each school's data protection policy and the Department's Retention Schedule.

5.11. Government account details must not be used for personal purposes.

5.12. Do not store the only copy of Government information on removable media (e.g. flash drive or USB drive) or in a location that is not backed-up.

5.13. The distribution of Government information must be limited to only those who need access.

Reporting concerns

5.14. Report any actual or suspected modification to ICT facilities using the incident reporting procedures.

5.15. For any breach of this policy, please refer the matter to the Department's SIRO or DPO immediately.

5.16. In the following circumstances, GTS must be notified to arrange a secure wipe of ICT facilities:

- Upon becoming aware of any loss or theft of ICT facilities;
- When ICT facilities are being replaced, upgraded or sold; or
- When a member of staff's employment with the Government ceases.

5.17. Where it is believed that ICT facilities or personal devices have been used for illegal activities, schools must refer the matter to the police and any other relevant agencies.

5.18. If a matter raises safeguarding concerns, it must be brought to the attention of the school's Designated Safeguarding Lead and escalated in accordance with the school's Safeguarding/Child Protection Policy.

Associated Resources

Safeguarding and Child Protection Policy

Nudes and Semi-Nudes Guidance

Mobile Phone Policy

Version Control and

Version	Author	Date	Changes
V1	Policy Hub	January 2025	N/A