# **DEPARTMENT OF EDUCATION, SPORT AND CULTURE**

RHEYNN YNSEE, SPOYRT AS CULTOOR





**Mobile Phones and Smart Devices** 

**Policy for Schools** 

### **Glossary**

**Authorised staff** are members of staff, from the school, Department or GTS, who are authorised to use school phones.

**Child Protection** is part of the safeguarding framework and describes the actions we take to protect children from harm and maltreatment. It is reactive to situations where we are concerned that significant harm has been or might be caused to a child and prescribes the actions that must be taken.

**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.

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

**Safeguarding** is a proactive framework of rule, boundaries, acceptable behaviours, norms and expectations aimed at:

- Protecting children from maltreatment;
- Preventing impairment of children's health or development;
- Ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and
- Taking action to enable all children to have the best outcomes.

**School(s)** means any primary or secondary school that is a "provided school" or "maintained school", as defined by sections 2(5)(a) and (b) of the Education Act 2001.

**SIRO** means the Department's Senior Information Risk Owner.

**Smart device** means mobile phones, iPods, iPads, tablets and similar devices including associated devices such as headphones, Airpods and smart watches.

**Staff** means any full-time or part-time staff at a school or from the Department and includes volunteers and governors.

**Work phone** means a mobile phone that has been provided to a member of staff for work purposes.

# **Contents**

Summary	3
About this policy	
Who is this document for?	3
Key points	3
Effective date	3
Policy	4
1. Roles & Responsibilities	4
2. Use of Smart Devices by Staff	4
Personal smart devices	4
Data protection	4
Safeguarding	4
Using personal smart devices for work purposes	5
Work phones	5
3. Use of Mobile Phones and Smart Devices by Learners	5
Confiscation	6
Searching a device	6
4. Use of Mobile Phones by Parents/Carers, Volunteers and Visitors	7
Contractors	7
Supervising school trips	7
Contacting their child	7
5. Loss, Theft or Damage	8
Version Control	9

### **Summary**

#### **About this policy**

The Department recognises that mobile phones and smart devices are an important part of everyday life for learners, parents/carers and staff, as well as the wider school community.

This policy aims to:

- Promote, and set an example for, safe and responsible smart device use;
- Set clear guidelines for the use of smart devices by learners, staff, parents/carers and volunteers; and
- Support the Department's other policies, and those of each school, especially those relating to safeguarding and child protection, acceptable use, and behaviour and relationships.

#### Who is this document for?

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

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

#### **Key points**

This policy addresses some of the challenges posed by smart devices in school, such as:

- Risks to child protection;
- Data protection issues;
- Potential for lesson disruption;
- · Risk of theft, loss, or damage; and
- Appropriate use of technology in the classroom.

This policy should be read in conjunction with any other relevant policies issued by the Department or schools, such as acceptable use, safeguarding and child protection, and behaviour / relationships.

#### **Effective date**

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

## **Policy**

#### 1. Roles & Responsibilities

- 1.1. All staff are responsible for enforcing this policy.
- 1.2. Volunteers, or anyone else otherwise engaged by the school, must alert a member of staff if they witness, or are aware of, a breach of this policy.
- 1.3. The head teacher of each school is responsible for the implementation of this policy.

#### 2. Use of Smart Devices by Staff

#### Personal smart devices

- 2.1. Staff are not permitted to make or receive calls, or send texts or messages, during contact time or whilst in the presence of learners. Use of personal smart devices must be restricted to non-contact time, and to areas of the school where learners are not present (such as the staffroom).
  - If staff wish to wear smart watches, they must ensure that notifications are silenced and use is minimised during contact time and whilst in the presence of learners.
- 2.2. There may be circumstances in which it is appropriate for a member of staff to have use of their personal smart device in the presence of learners. For instance:
  - For emergency contact by their child or their child's school;
  - In the case of acutely ill dependents or family members; and
  - For 'special arrangements', to be agreed with the head teacher and decided on a case-by-case basis.
- 2.3. If special arrangements are not deemed necessary, school staff can use the school office number as a point of emergency contact during contact time.

#### Data protection

2.4. Staff must not use personal smart devices to process personal data of any school learners, or any other confidential school information, including entering such data into generative artificial intelligence (AI) tools such as chatbots (e.g. ChatGPT and Google Bard), unless it is using an application supported by GTS, such as email and Microsoft Teams.

#### Safeguarding

- 2.5. Staff must refrain from giving their personal contact details to parents / carers or learners, including connecting through social media and messaging apps.
- 2.6. To reduce the risk of unwanted contact by parents / carers or learners, staff should avoid publicising their personal contact details on any social media platform or website.

2.7. Staff must not use their personal smart devices to take photographs or recordings of learners, their work, or anything else that could identify a learner. If it is necessary to take photos or recordings as part of a lesson/school trip/activity, this must be done using school equipment.

#### Using personal smart devices for work purposes

- 2.8. In some circumstances, it may be appropriate for staff to use personal mobile phones for work purposes. Such circumstances may include, but are not limited to:
  - Email and Microsoft Teams or other applications supported by GTS;
  - When on duty, in case of emergency where support may be required;
  - Emergency evacuations;
  - Supervising off-site trips; and
  - Supervising residential visits.
- 2.9. In these circumstances, staff will:
  - Use their smart devices in an appropriate and professional manner, in line with our staff code of conduct;
  - Not use their smart devices to take photographs or recordings of learners, their work, or anything else which could identify a learner; and
  - Where incidents have occurred onsite, refrain from using their personal smart devices to contact parents/carers. Where practicable, contact with parents/carers should be made via the school office.
    - However, if an incident has occurred offsite, it may not be practicable to contact parents / carers via the school office. In such an instance, it may be necessary to use a personal smart device.
- 2.10. Before personal devices can be used to access or store Government information, approval must first be obtained from the Department SIRO, and only GTS-approved solutions may be used, along with any security measures that are provided to you.

#### Work phones

- 2.11. Work phones may be provided to specific members of staff and must not be accessed by anyone other than the authorised user.
- 2.12. Use of work phones must be in accordance with the Department's Acceptable Use policy and the <u>Isle of Man Government Acceptable Use Handbook</u>.

#### 3. Use of Mobile Phones and Smart Devices by Learners

- 3.1. Learners are permitted to bring their smart devices to school but must keep them turned off and safely stored away during lessons and whilst traveling through the school.
- 3.2. Learners who choose to bring their smart devices to school do so at their own risk. Neither the Department nor the school is liable if a learner's smart device is lost or damaged on school premises.

- 3.3. Smart devices may be used in certain circumstances, when arrangements are approved by the head teacher, such as supporting the operation of a medical device (e.g. glucose monitoring).
- 3.4. Exception may also be made where a family anticipates that they may need to contact a learner in an emergency. In such a case, arrangements can be made with the school for the learner to have their smart device available at the relevant times.
- 3.5. Any breach of this policy must be dealt with in accordance with the schools' behaviour / relationship policy.

#### Confiscation

3.6. Under section 21B(2)(d) of the Education Act 2001, schools may seize and detain 'any article, the possession or use of which by a learner is forbidden under any rule of discipline for the time being in force at the school'.

This Policy is a 'rule of discipline' which is in force at schools, meaning that schools may seize smart devices where their possession or use is in contravention of school policy. However, schools must have established processes for:

- Escalation to confiscation (within the school's Behaviour / Relationships Policy);
- The safekeeping of confiscated smart devices; and
- Arrangements for learners or their parents / carers to collect confiscated smart devices at an appropriate time.
- 3.7. Before confiscating a smart device, and when deciding how long to confiscate for, school should consider whether the learner requires the smart device for other purposes, such as medical monitoring.

#### Searching a device

- 3.8. Members of staff may search the data and files of a smart device if they have a reasonable suspicion that data or files on the smart device could:
  - Cause harm;
  - Undermine the safe environment of the school;
  - Disrupt teaching; or
  - Be used to commit an offence.
- 3.9. However, if a member of staff suspects that they may find an indecent image of a child, the member of staff must:
  - Not intentionally view the image;
  - Confiscate the smart device; and
  - Refer the incident to the Designated Safeguarding Lead (DSL).

Further information and guidance is available in the <u>Department's Safeguarding and Child Protection Policy</u> and the Nude or Semi-Nudes Guidance, and the relevant school's Safeguarding / Child Protection Policy.

3.10. If staff find data or files that they believe the continued existence of could cause harm to anyone, they may delete the data or files.

- 3.11. Where staff believe that criminal behaviour has occurred, they must inform the DSL who will refer the matter to the police and/or other relevant agencies. Such conduct could include, but is not limited to:
  - Sexting;
  - Recording intimate images without consent;
  - Consensual and non-consensual sharing of nude or semi-nude images and/or videos;
  - Threats of violence or assault; and
  - Abusive calls, emails, social media posts or texts directed at someone on the basis of someone's ethnicity, religious beliefs or sexual orientation.

Further information and guidance is available in the documents linked in point 3.8.

#### 4. Use of Mobile Phones by Parents/Carers, Volunteers and Visitors

- 4.1. Parents/carers, visitors and volunteers (including governors) must adhere to this policy as it relates to staff if they are on the school site during the day.
- 4.2. This means:
  - Not taking pictures or recordings of learners, unless it's a public event, or of their own child;
  - Not taking pictures or recordings of staff, without prior consent;
  - Using any photographs or recordings for personal use only, and not posting on social media without consent; and
  - Not using phones in lessons, or when working with learners.
- 4.3. Parents/carers, visitors and volunteers will be informed of the rules for mobile phone use when they sign-in at reception or attend a public event at school.

#### **Contractors**

4.4. Contractors may be required to use smart devices to fulfil their work duties; however, they must not record or take images of any persons on the school premises.

#### Supervising school trips

- 4.5. Parents/carers or volunteers supervising school trips should not take photos or recordings of learners, their work, or anything else which could identify a learner.
- 4.6. Parents/carers or volunteers supervising trips are also responsible for enforcing the school's policy for learners using their phones, as set out in section 3 above.

#### Contacting their child

4.7. Parents / carers should use the school office as the first point of contact if they need to contact their child during the school day.

4.8. Parents / carers should not try to contact their child on their personal smart device during the school day, unless they have made prior arrangements with the school.

#### 5. Loss, Theft or Damage

- 5.1. Learners bringing phones to school should ensure their smart devices are appropriately labelled and stored securely when not in use.
- 5.2. Learners should secure their personal smart devices, with the use of passwords or pin codes, to protect access to the smart device's functions.
- 5.3. Staff should secure their personal smart devices to prevent them from being accessed in the event that they are lost on school premises.
- 5.4. The school accepts no responsibility for mobile phones that are lost, damaged or stolen on school premises or transport, during school visits or trips, or while learners are travelling to and from school.
- 5.5. Lost smart devices should be handed into the school Reception. Staff will then make efforts to contact the owner.

# **Version Control**

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