Mont Nicolle School

1. Users and Devices

a. This policy applies to all staff, pupils and guests including parents and volunteers, and applies to all mobile devices used within school.

b. Devices covered by this policy include smartphones, tablets, laptops, eBook readers etc.

2. Purpose

a. Mont Nicolle's School is committed to the correct and proper use of mobile devices in support of its administrative and educational functions and in its ambition to enhance teaching and learning.

b. It is expected that all users will act responsibly to protect their online profile and respect the privacy of others at all times.

c. School-owned devices are provided for exclusively educational use, regardless of whether they are used at school or elsewhere.

d. The inappropriate use of mobile devices could expose the school to risks including child protection, data protection and digital safeguarding matters, and as a consequence disciplinary or legal issues. The purpose of this policy is to define acceptable, safe and secure standards for the use and management of mobile devices within the school.

e. This policy is mandatory and by using any mobile devices within the school building or grounds that are owned by staff, volunteers, visitors, or that may be leased or owned by the school; users are agreeing to abide by the terms of this policy.

3. Scope

a. This policy represents Mont Nicolle's School's position and sits within the policy documents as defined by the Department for CYPES, regarding safeguarding and Child Protection, Data Protection and Online Safety. The policy applies to all mobile devices which are brought onto the site regardless of whether they are owned or leased by the school or not.

b. The school has a responsibility to identify the procedures that they will employ to safeguard users against the potential ramifications arising from the misuse of mobile devices that facilitate access to wireless networks from within Government of Jersey sites. As a consequence, all staff, visitors and volunteers have a responsibility to follow the agreed policy.

c. The monitoring and review processes of this policy are the responsibility of the Headteacher, Digital Safeguarding Officer and Designated Safeguarding Lead.

d. All exceptions to this policy must be authorised by the Headteacher, who will take advice from the Digital Safeguarding Coordinator at CYPES if required.

4. Connectivity

a. Mobile devices must only connect to the school's network via the wireless network. BYODs must not be plugged into network sockets or desktop USB ports unless this action has been specifically approved in advance.

b. Staff, students and visitors wishing to connect a mobile device to the school's wireless network must first ask permission from the Headteacher, ICT Subject Leader or ICT Technician. In connecting to the network, they agree to follow the Responsible Use Policy – see Appendix 1.

All use of the school network is monitored and by connecting, users give their consent for this monitoring to take place.

c. Once a device has been enabled, users must only access the wireless network using their own log-in details. Users must not share their usernames and passwords.

d. Adults, who have their own internet account for their mobile device using a third party network (3G/4G), may access this within the staffroom environment or one of the school offices for their own personal use. It is unnecessary and inappropriate that staff, volunteers or visitors should access an e-unsafe network in the presence of pupils of the school whilst on supervision duties or in classrooms, where pupils may require access to their belongings. This would constitute an unnecessary risk as it is possible to access the internet safely within the school using the network facilities provided.

e. Devices that are found to be compromised in some way may be denied access to the school's network (denial of access may be triggered automatically by the web filter).

f. If software is installed on a personal device (whether school - or home-owned) to facilitate connection to a school's network, or for other purposes, then all of that software's capabilities must be disclosed to the device owner.

g. All areas in the school have been fitted with telephones; staff are expected to use these to communicate for business purposes, rather than to use their own personal mobiles, which may place their own personal details at risk. Personal calls should not be taken in the classroom on mobile phones, during teaching hours, staff and volunteers are not expected to take personal calls, other than through the school office. Staff should alert the office to any expected phone calls of a sensitive nature, so that these may be dealt with appropriately.

h. There may be exceptional circumstances when mobile phone could be used in the presence of pupils, e.g. on a school visit where a Health and Safety issue arises and support is required either by emergency services or school staff.

i. Although there are many e-learning benefits that may be accrued by allowing home-owned computers to be used on site there is also a risk that they may bring unacceptable content or facilitate inappropriate uses on-site. These risks may exist regardless of whether or not home-owned computer devices are connected to school networks. Home-owned computers are not allowed into the school unless they are subject to filtering, monitoring and logging that is equivalent or identical to that which applies to school owned computers. At the present time, BYOD is not being implemented at Mont Nicolle School.

j. School-owned staff laptops and tablets can be scrutinised at any time if there is a concern.

k. Any person who wishes to bring a home-owned computer into the school must comply with all the conditions imposed above. If there is reason to believe there are digital-safeguarding concerns about a home-owned computer, then the device should be inspected and if the user does not agree to such inspection then the device must be immediately removed from the site. A home-owned computer that has been the cause of a digital safeguarding concern must not be brought back on-site until specific permission has been granted for this to happen: it may be a condition of such permission that additional monitoring software is placed on the home-owned computer and is allowed to function unencumbered for the entire time when the device is on-site.

l. Mobile devices often incorporate image-capture features that can be used to record stills or videos, which can be a valuable tool for teaching and learning. However, there is also the potential for misuse in the form of ridiculing or bullying members of staff or pupils. Any

inappropriate use of images should be reported to the school's senior leadership team and will be dealt with in accordance with the school's Anti-Bullying Policy.

m. Users are requested to ensure that they only use school-owned devices for taking digital images, and that all images are stored on the school network. Occassionally, photographs are taken for social media. Photographs should not be stored on mobile phones or home computers to safeguard individuals and secure best practice.

n. Cloud-based storage should not be used unless this has been risk-assessed by the school's Digital Safeguarding Lead (DSL) or ICT Lead.

o. If any visitor, volunteer or member of staff is observed taking photos this should be reported to the school's DSL staff in line with the 'Procedures for Managing Allegations Against a Member of Staff'. This also applies to volunteers within the school. Visitors should not be taking photos unless they have been given permission by the Headteacher and are being guided by the 'Acceptable Use of Photos and Videos' Policy and Data Protection Policy.

5. Software/apps

a. All software and apps to be used for teaching and learning purposes should be approved by the Digital Safeguarding Lead. Any web-based applications must be fully risk-assessed before use in school. The ICT technician will be responsible for purchasing and installing new software and apps, under the guidance of the ICT Subject Leader and Digital Safeguarding Lead.

b. Teachers may install software on their school-owned devices for educational use, but all software should come exclusively from trusted sources: ideally users should consult with the school before installing any software.

6. Data Protection

Please refer to the school policy and also the CYPES Policy

7. Security and virus protection

a. All mobile devices (both school-owned and BYOD) that are used professionally by members of staff must be protected, by passwords or passcodes and these changed regularly.

b. School-owned devices that are supplied to members of staff must be maintained in their supplied state: they must not be "jailbroken" or "rooted".

c. All mobile devices must have up-to-date anti-virus and other security software (such as privacy protection applications) installed. No types of devices should be exempted from the need for virus/privacy protection software.

d. In the event of a school-owned device being lost, the person to whom the device was loaned must inform the school as quickly as is reasonably possible. Lost school-owned devices may be wiped-clean of all data (if provisioning allows this): the assignee agrees that this may include all personal-use information too.

8. Right of inspection

a. The on-site use of all mobile devices, both home-owned and school-owned, is subject to the

user granting the school a right of inspection on request.

b. Requests for inspection can only be made in response to a specific cause for concern. Inspections will be carried-out only by designated senior members of staff. Pupils are entitled to insist that a parent is present throughout any inspection. Members of staff are entitled to insist that a union representative is present throughout any inspection.

c. Refusal to allow an inspection when one is requested may result in withdrawal of consent for the device to be used on-site.

d. School-owned devices must always be used in a manner that is consistent with the purposes for which they are provided: if inappropriate use is discovered during an inspection then disciplinary action may be taken.

January 2023

This policy is subject to regular review and will be updated at the latest by September 2023