VERITAS

Dominican College

Pupil USE of Mobile Technology

Bring Your Own Device Policy

Contents

1. Introduction

Dominican College is committed to innovating with educational technology to enhance communication, teaching and learning within our school community. We embrace the opportunities that mobile device (MD) technology has presented us with and permit the use of a MD in a manner consistent with the established teaching and learning objectives of the School. We also recognise and encourage the use of mobile technology for educational purposes at home.

Once the attached pupil and parental consent form is signed this policy applies to all pupil users who have been given permission by the Principal to 'Bring Your Own Device'[1] (BYOD) to school. It applies to all MDs used by our pupils, wherever they are physically located - within the School, used in a Partner School or at home. It is intended to complement the School's wider ICT Policy, the Acceptable Internet Use Statement and its E-safety Policy. Due to the nature of information and communications technology the policy will undergo periodic review and as such the School reserves the right to amend any sections or wording at any time.

The following details define the proper use of the device in school and out of school hours.

2. General MD Terms

a. Your MD – Media, Apps, Communication, Connectivity, Backing-up and Care
Any pupil who uses a MD in School or in any Partner School must sign up and adhere to the terms stated in this Policy as well as other relevant Acceptable Use Policies (AUPs), e.g. E-safety Policy, ICT Policy, Acceptable Internet Use Statement, etc. The School maintains the right to selectively filter internet content and manage the use and connection of MDs to the school network in line with its E-safety Policy.

It will be expected that any MD being used in school will have all personal files (e.g. photographs, videos, text, etc.) and inappropriate Apps removed. It is recommended that any personal files not associated with school use are backed-up (e.g. external hard drive or cloud storage) or deleted before first use in school. Personal files, images, videos, text, music, games and Apps (e.g. social media) should not be accessed (even from cloud storage) while on the school premises. In terms of communication; no telephone calls, video conferencing, text messages or other forms of personal messages are permitted. Pupils may, for school related activities, communicate via their C2K email but only when permitted to do so by a member of staff. If a pupil needs to communicate with a parent or guardian this should be done in the traditional way via the Office and after permission has been sought and granted from a member of staff. Any pupil accessing non-school related media or communicating with others outside the parameters of this BYOD Policy will be subject to the School's disciplinary and E-safety Policy sanctions.

In terms of connectivity, all pupils given permission to use their MD in school will connect to the C2K wifi network. A designated teacher will instruct each pupil on how to install the C2K profile onto their MD, which is necessary for the wifi to operate. Once installed each pupil accesses the secure C2K wifi using their unique C2K username and password. This enables a managed wifi system to be maintained with each MD logged and digital footprint traceable.

---

[1] 'Mobile Device' in the context of this policy applies to tablets and laptops. It does not include mobile/smart phones.

Pupils are not permitted to use their mobile data (e.g. 3G or 4G) nor must they ever use their MD as a personal hotspot for themselves or others.

It is the responsibility of each pupil to make backups of their school documents, photographs, videos, etc. on a regular basis. A pupil will not be permitted to use a MD in school unless they have signed this BYOD Policy. Please note than on occasion MDs may be subject to inspection, to ensure they comply with this policy as well as other acceptable use policies, by an appropriate member of staff (e.g. E-safety Coordinator, Senior Teacher or ICT technician). Requests to add MDs onto the school network must be made via a senior teacher or a designated teacher.

The School disclaim all responsibility for damage, loss or theft for any personal MD brought into school. It is recommended that MDs brought into school are not left unattended and are insured by each pupil or by a parent/guardian for their replacement value, either by specialised MD insurance or generic household policies (i.e. protect devices/valuables away from home).

b. Taking Care of Your MD
• Pupils are responsible for the general care of the MD.
• MDs must never be left unattended or in any unsupervised area.
• A protective case should be used with the MD and have sufficient padding to protect the MD from normal treatment and provide a suitable means for carrying the device within the School. MDs should always be within the protective case when carried.
• Avoid placing too much pressure and/or weight (such as folders and workbooks) on the MD screen. The MD screens can be damaged if subjected to rough treatment. The screens are particularly sensitive to damage from excessive pressure.
• Avoid excessive movement on school bags containing MDs.

c. Using Your MD at school

i. General Use
• MDs, which are granted permission for use should ONLY be used for school use and when supervised by a member of staff (e.g. Sixth Form Study Hall, Library, Art, ICT, Music and during timetabled lessons). Therefore, during break and lunchtime MDs should NOT be used.
• School messages, announcements, planners, calendars and schedules may be accessed using the MD.
• It is recommended that MDs should have a suitable case to protect the device. This case must be appropriate for school use. Where the appropriateness of the MD case is questioned the E-safety Coordinator and senior staff will have the final say on the appropriateness of the case.
• All MDs must be clearly and securely marked (e.g. on the case or outside of the device) in the unlikely event it is misplaced.
• All lock screen and wallpaper images will be suitable in line with the Code of Conduct.
• Each device is governed by this policy in conjunction with the School's Code of Conduct, the ICT Policy, the Acceptable Internet Use Agreement and the E-safety Policy. These policies are subject to change and they govern all security and restrictions applied school wide to all devices.

ii. Use During Lessons

- If teachers and pupils have agreed in advance and made arrangements to use MDs during lessons pupils must bring their MD (fully charged) into school when required. Failure to bring the MD will be treated the same as any other piece of equipment. Pupils may be subject to departmental or whole school sanctions in line with the School's Positive Behaviour Policy.
- Subject departments or members of staff may develop an MD 'Users Charter' for acceptable use during lessons. These will be in keeping with this Policy and other school policies and pupils must abide by these.
- If pupils fail to bring their MD to class, following a prior agreement with their teacher, they are responsible for getting any assignments or coursework completed within the agree timeline. Spare MDs will not be available to pupils who forget to bring their MD to school or who fail to charge their MD.
- MD malfunctions are not an acceptable excuse for not submitting work. Therefore, pupils should routinely back-up all work using facilities such as iCloud, Dropbox or Google Drive.
- At all times, the class teacher's decision is final regarding use, or non-use of any MD, collectively or individually.

d. Passwords and Access IDs

- MDs should be password protected. Pupils are prohibited from sharing this password with anyone else except their parents or as requested by a senior teacher.
- Pupils may not attempt to access other pupils MDs by 'guessing' or trial and error password attempts.
- Passwords should be changed regularly.
- Most MDs will require users to have a personal username or ID to allow access to online App stores. These user IDs should all be established before any device is used in school.
- User IDs should be kept secure to the owner, and it is the responsibility of the pupil to recover any lost or forgotten passwords.
- Pupils who are authorised to use a MD in school must be the sole user with full responsibility for the device. Some MDs (mainly android) are capable of allowing multiple account holders with separate Access IDs (i.e. shared access to the device). Currently these MDs are not permitted for use in school. Each MD must have only one user and one Access ID, this Access ID must be associated with pupil using the device.
- It is also up to each user to monitor their own account (e.g. Apple or Android) as some accounts may charge for Apps, media, etc.)
- If pupils or parents are purchasing or dedicating a MD solely for school use then it is recommended that pupils set the device up primarily for school use, e.g. name the device after the pupil's C2K username, use the pupil's C2K email to register a new Access ID and establish the primary email on the device as the C2K email.

e. Audio-Visual content

i. Photographs and Images (still or moving)

- Photographs/Images stored on the MD will be in accordance with the School's Code of Conduct. The School reserves the right to randomly check any MD for unsuitable content.
- No images or video material taken in school may be uploaded from any device to social networking sites.
- Recording of classroom teachers is prohibited unless specifically permitted by the class teacher.

5

ii. Sound, Music, Games or Apps

- Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
- Gaming on MDs whilst in school is strictly prohibited.
- Apps on the MDs must not violate any terms of this policy or any other AUPs.
- Recording of classroom teachers is prohibited unless specifically permitted by the class teacher.

f. Home use

- Pupils are free to use their MD at home (or outside of school) and set up wireless networks on their MDs to assist them with homework's, coursework, controlled assessment, etc. It is the responsibility of the Parent/Guardian to monitor and oversee MD use outside of school.
- Our school website (http://www.dominicancollege.org.uk/) has links for parents/guardians regarding e-safety.

g. Procedure for reloading software

- If technical difficulties occur or illegal software is discovered, the MD may need to be restored from back-up. The school does not accept responsibility for the loss of any software or documents deleted due to a re-format and re-image.

h. Software Updates

- Upgrade versions of licensed Apps are available from time-to-time. Pupils will be expected to download all updates prompted by Apple, Google, etc.
- Upgraded version of the operating system may also be available. However, pupils should ensure all work is backed-up before updating.

i. Software and Apps (*only applicable if a MDM is used*)

- The School may ask pupils to install a Mobile Device Management (MDM) App or profile. If this occurs each pupil will be shown how to register the MD with the MDM platform. MDM solutions allow multiple MDs to be managed at the same time and if requires send notifications or 'push' documents, files, other media or Apps. Pupils must always accept any media or action any notification sent via the MDM system.
- Periodic checks of MDs may be made to ensure that pupils have not removed required Apps.
- The School's remote management system can monitor all apps that are added to each MD and may be flagged if inappropriate Apps are added. On occasion pupils may be asked to remove inappropriate Apps.
- Normally any 'pushed' Apps remain the property of the School and may be removed when the pupil leaves the school or no longer requires the App.

3. Acceptable Use

In addition to the School's ICT Policy and Acceptable Internet Use Statement, the School permits the use of a MD in a manner that supports the School's aims and objectives and is in line with all School Policies. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the user terms and conditions named in this policy, privileges may be terminated, access to the School's network may be denied, and the appropriate disciplinary action shall be applied in line with the School's Positive Behaviour Policy.

a. PARENT/GUARDIAN RESPONSIBILITIES

Parents are expected to talk to their children about the values and standards that they should follow on the use of the internet just as they do on the use of all media information sources such as television, telephones, movies, radio, iBooks etc. (i.e. e-safety). Parents and pupils should familiarise themselves with the details of any MD Insurance Plan in case of accidents, theft or misuse. If payment details (e.g. credit card) have been associated with the users Access ID then it is essential that both parents and pupils review this regularly and are aware if purchases are made. The School will not be held liable for any purchases made.

b. PUPILS' RESPONSIBILITIES ARE TO:

• Use MDs in a responsible and ethical manner.
• Obey general School rules concerning behaviour and communication that apply to MD and computer use.
• Follow and accept any departmentally agreed MD rules, which will be communicated to pupils via their class teacher.
• Only use their MD when and where a member of staff permits. Break and Lunchtime are not acceptable times to use a MD (unless working alongside a teacher).
• Use all computer resources in an appropriate manner so as to not damage school equipment.
• Turn off and secure their MD after they are finished working to protect their work and information.
• Report any email containing inappropriate or abusive language or if the subject matter is questionable.
• Where available pupils should install an App or software that allows them to remotely find their device (e.g. for Apple devices "**Find My iPad**" and for Android devices "**Android Device Manager**").
• Pupils must have their own, personal Access IDs.
• For all school-based communication pupils must use their C2K email address (e.g. aexample123@c2kni.net).
• Back-up and charge their MD on a regular basis and bring it every day to school, if MD use has been agreed in advance with their teacher(s).

c. Pupil Activities Specifically Prohibited

In addition to the guidance outlined in the School's ICT Policy, Code of Conduct and Acceptable Internet Use Agreement pupils are **not** permitted to do the following while in school, at a partner school/institute or representing the school:

• Illegally install or transmit copyrighted materials.
• 'Jailbreak' their MD.
• Use another pupil's MD.
• Leave their MD on the School premises overnight, unless it is given to the IT technician or designated teacher.
• Send or display offensive messages or material.
• Use obscene language or content.
• Cause damage to the computer systems or computer networks.
• Use other people's passwords.
• Trespass in others' folders, works or files.
• Download illegal content or material which is suspicious.
• Have unsuitable images displayed as part of the 'locked screen' or general background.
• Upload any material (e.g. audio, photo or video content, etc.) taken in school to any social networking sites or blogs.

d. Legal Propriety
• Pupils should comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If a pupil is unsure, she should ask a teacher or parent.
• Use or possession of hacking software is strictly prohibited and violators will be subject to sanctions. Violation of the law may result in criminal prosecution or disciplinary action.

4. Inappropriate Use of Your MD

a. Disciplinary measures
If a pupil violates any part of the BYOD policy, the following sanctions will apply:

•**1st Offence (Minor)** – Pupil(s) will have their MD left at Reception for safe keeping. Pupils will then have to collect the MD at the end of the school day. Details of 'Check-In' and 'Check-Out' will be recorded and a letter may be sent home with a warning regarding future use of the MD.

•**2nd Offence (Minor)** – Pupil(s) will have their MD left at Reception for safe keeping. Parent/Guardian's will have to collect the MD at the end of the school day. Details of 'Check-In' and 'Check-Out' will be recorded.

•**3rd Offence (or Major)** – Pupil(s) will have their MD left at Reception or given to a Senior Teacher for safe keeping. Loss of MD and privileges for a length of time will be determined by the Senior Teacher. Depending on the nature of the offence the Principal (and other authorities) may be informed and a suspension may ensue.

Any pupil who persistently refuses to co-operate or violates any aspect of the provisions of the BYOD Policy or the other AUPs may face other disciplinary action deemed appropriate in keeping with the School's Positive Behaviour Policy.

Violations may result in disciplinary action up to and including suspension/expulsion for pupils. When applicable, law enforcement agencies may be involved.

b. A pupil will be required to hand over their MD to a member of staff if:
• There is a suspicion that the MD has unsuitable material stored on it.
• A pupil has disrupted a lesson through improper use of a MD.
• A pupil has misused their MD to take photographs/video on the school premises which they have not received permission to do so.
• The MD or any of its features has been used for any form of bullying.
• Games are being played on the MD during school time.
• The MD has been used to breach any school rule/policy and general well being of staff and pupils.

5. BYOD: Pupil and Parental Consent

Please sign in the appropriate space below and return the bottom part of this page to **your tutor**. By signing the pupil and parental consent form you are agreeing to abide by this policy the Acceptable Internet Use Agreement, ICT Policy and the E-safety Policy; which all work with in conjunction with the School's Code of Conduct. This agreement lasts until the pupil's enrolment is terminated through transferral, withdrawal, suspension or expulsion during, or at the end of, a school year.

✂ - - - - - - - - - - - - - - - *Please retain this policy and ONLY return the signed consent part below* - - - - - - - - - - - - - - -

BYOD: Pupil and Parental Consent Form

Pupil Signature: _____ **Date:** _____

Parent/
Guardian Signature: _____ **Date:** _____

By signing the pupil and parental consent form you are agreeing to abide by this BYOD policy the Acceptable Internet Use Agreement, ICT Policy and the E-safety Policy; which all work with in conjunction with the School's Code of Conduct. This agreement lasts until the pupil's enrolment is terminated through transferral, withdrawal, suspension or expulsion during, or at the end of, a school year.