Sir William Borlase's
Grammar School

# Digital Device Code of Conduct (Formerly Mobile Phone Code of Conduct)

Senior Leader Review Lead : Deputy Headteacher, James Simpson

Approved: October 2021

For review: October 2022

For review by: PDW /FGB

*Inspire*
*Empower*
*Shape The Future*

## 1. Introduction

Students and their parents/carers must read and understand the Digital Device Code of Conduct as a condition upon which permission is given to bring digital devices to school.

The school makes a distinction between personal digital devices such as smartwatches and smartphones and the digital learning devices - a laptop, Chromebook or tablet with integrated keyboard - which all Borlase students are expected to bring to school.

It is well understood that all digital devices can be sources of distraction as well as powerful tools to facilitate learning. The school's learning environment should be a place where students and teachers can make productive use of the benefits of digital devices while minimising their potential for distraction or harm.

## 2. Digital learning devices

Borlase students are expected to have access to their own wifi-capable device to support learning at school or in the Borlase@Home learning environment necessitated by the shutdown of schools caused by the coronavirus.

This expectation gives teachers the flexibility to make effective use of IT without the need to leave their teaching classroom, facilitating more effective student-student and student-teacher collaboration.

All Borlase students should bring to school a WiFi-capable digital learning device that meets the following specifications:

- is suitably lightweight and robust enough to survive being carried around all day (although we strongly recommend that students bring their device in a protective case)
- is equipped with a genuine keyboard (i.e. tablet devices such as iPads must be accompanied by a folio-type tablet case with in-built keyboard)
- has a battery life sufficient to last the full school day

Students are expected to use their digital learning devices responsibly, following the school's clear Acceptable Usage statement (Appendix 1) that all students agree to by accessing our wifi network. Misuse of digital learning devices is not acceptable and will be sanctioned according to the school's Behaviour for Learning policy.

## 3. Personal digital devices

### a. School policy applicable to all students

Sir William Borlase's Grammar School recognises that communication through personal digital devices is part of everyday life for families, socially, academically and professionally. It is the responsibility of the school to ensure that students and staff understand their responsibilities with respect to personal digital devices so that everyone can feel safe at school and outside school.

There is significant evidence that indicates that access to personal digital devices increases the potential for bullying, is a cause of anxiety related to social media, and has a negative impact on achievement. Young people can feel under pressure to use digital devices where they have access to it.  Sir William Borlase's Grammar school supports young people's right to be disconnected from social media during school hours.  Our school wifi network does not allow access to social media sites (e.g. Facebook) and students are not expected to be accessing social media sites for personal or social purposes during the school day.

Parents/carers should be aware that if their child takes a personal digital device to school, it is assumed household insurance will provide the required cover in the event of loss, damage or theft. The school will not accept responsibility for costs incurred due to its use.

**It is the responsibility of all students to ensure that they do not use or handle their personal digital device until they have left the school premises.   During the course of the school day, personal digital devices should be turned off and kept out of sight either in a securely locked locker, in a zipped or buttoned blazer or jacket pocket or in a bag.**

Parents/carers are reminded that in cases of emergency, the school office is the first point of contact or Matron for medical issues and office staff can ensure your child is reached quickly and assisted in any relevant way. Passing on messages through school reception also reduces the likelihood of inadvertently disrupting lessons.

Pupils have access at any time of the day to a telephone in reception, with matron or their Key Stage office if they need to contact parents for an emergency or personal reason.

Using personal digital devices to bully or threaten other students is totally unacceptable. In some cases it can constitute criminal behaviour. If the use of technology humiliates, embarrasses or causes offence, it is unacceptable regardless of whether 'consent' was given.

It is forbidden for students to join together to target any student, individual or member of staff; to use their mobile phone to take videos/images in order to denigrate and humiliate an individual. Sharing, sending or uploading images/videos to other students or individuals, or making them publicly available is strictly prohibited. This also includes using mobile phones to photograph or film any student, individual or member of staff without their consent. It is **a criminal offence** to use a mobile phone to menace, harass or offend another person and almost all calls, text messages and emails can be traced.

It is a **criminal offence** to take sexually explicit photos of others or yourself and send them to others. If a student receives an explicit photograph or is requested to send one they should report this immediately to a member of their Key Stage Team, a member of the Safeguarding Team, or directly to the police.

It is unacceptable to take a picture of a member of staff without their permission. In the event that this happens the student will be asked and expected to delete those images. Examples might include during the school day,  at a school function or going home.

All digital devices are banned from all exams by JCQ. Any student found in possession of a personal digital device during an exam will have their paper disqualified. Such an incident may result in all other exam papers being disqualified. JCQ requirements apply to all internal school assessments / exams. These are JCQ rules and schools must enforce them.

### b. Exceptions

The school recognises that some students choose to wear a particular type of personal digital device: a smartwatch such an Apple Watch. It should be understood that the wearing of such a device is permitted, but *only for the purpose of using it as though it were* ***not*** *a smartwatch.* The use of a smartwatch as a mobile phone or messaging device or to access the internet, apps or games is not permitted and would be treated as equivalent to using a smartphone.

The school recognises that some of the tools available in personal digital devices such as cameras and video recording and music libraries may be required in a small number of subjects - e.g. Music for GCSE or A level, the Dance curriculum. Teachers will state in advance when it is permitted for personal digital devices to be used in the classroom environment.

During extra- curricular activities, twilight lessons and after school clubs, personal digital device usage is at the discretion of the teacher leading the activity. They should be out of sight as usual unless the teacher agrees to the student using the personal digital device. Students should *not use cameras* or record themselves or others unless this is a specified learning activity within a specialist lesson.

The policy for usage of personal digital devices during educational activities, for example school trips, will be specifically directed by the staff trip leader. It is usual that for outdoor education experiences students operate without smart technology. For most school trips mobile phones are permitted to be used for emergency communication if requested.

Students must take responsibility to ensure phones are switched off during talks, theatre, concerts etc as they would during any school lesson.

### c. Specific exceptions for Sixth Form students

It is important firstly to note that Sixth Formers are *not permitted* to use personal digital devices in public areas around the school during the school day for any purpose, including listening to music; this includes canteen areas, playing fields, corridors and Cloisters at all times. It is very important that they set an example to the lower school in those shared spaces; public usage will result in confiscation.

The school recognises that Sixth Form students, who are developing into young adults, are able to leave the school site during lunch times. It is acceptable for them to access their mobile devices if they leave the school at this point in the school day.

Sixth Form students are permitted to use their phones during non contact periods, break and lunch in the area exclusively used by the Sixth Form: the Mimis cafe area.

Sixth Form students have access to a school phone with their Student Support Team, Matron or Reception if they need to make an emergency call or a call related to study/ university/ work experience etc ; they can use a small sixth form study office to make a call on their mobile phones if needed for these purposes, with staff permission.

Sixth Formers are permitted to have mobile phones on desks in supervised silent study; those students who find listening to music helpful must do so having gained permission from staff and using headphones.

## 4. Sanctions

Students who infringe the rules set out in this document will have their personal digital devices confiscated by school staff.

Confiscated personal digital devices will be taken to Reception, labelled with name and date and locked away securely. This will be logged in Reception and monitored by the relevant Head of Key Stage.

For a first and second confiscation in an academic term the student will be issued with 2 SIMS points and a lunchtime detention. The personal digital device can be collected by the pupil and signed out from Reception between 3.30 and 4.00 p.m.

A third confiscation in any academic term (persistent infringement) will result in the phone remaining in reception until parents/carers are able to collect it (between 8.00 a.m. and 8.30 a.m or 3.30 and 4.30 p.m.) and the issuing of a 3 SIM point after school detention.

Parents/carers will be notified so they can collect the phone on a convenient day and the phone will be held securely until they are able to do so.

# Appendix 1 - Acceptable Usage of ICT

The SWBGS acceptable usage policy is directed by UK laws and Statutory Guidance (see Appendices) and covers all devices, communications, and systems. It applies to all resources used within school premises and to all resources provided by SWBGS for staff, students and parents in and out of school.

As a term, resources includes but is not limited to:

Audio-visual equipment, Blogs, Cameras, webcams and Digicams, Computers, Computing software, E-mail, Fax, Instant Messaging/Collaborative applications, Internet and Intranet, Mobile devices i.e. laptops, mobile phones, chromebooks, PDA's etc… , Network, Printers, Remote access service, Scanners, Telephone or videophone, Text, Voicemail, Wikis

In accordance with relevant legislation you are advised that SWBGS has the capability to lawfully monitor and record your activity from any workstation or for any device using the school's facilities. This document informs the current regulations for the acceptable use of SWBGS's IT systems and displayed on the school website. You will be liable for any action deemed necessary by SWBGS as a result of contravening these regulations.

Please Note: Contents of this policy may be changed at any time to update for legislation or to protect the school

## Governance for all Users

The school network and Wifi systems are valuable resources that are available to all pupils and staff from their own devices and from most computers situated throughout the school. Due to the wide variety of uses by hundreds of users, a number of precautions have to be taken for your safety, the safety of others and to help ensure that all systems are kept available and in full working order:

Users are responsible for appropriate behaviour on the network and Internet, just as they are in a classroom or a school corridor. General school rules apply.

Access to the school network will be provided for you to carry out recognised school work (and social use within the limits which have been discussed in PSHCE and Assemblies AND provided such use is not conducted during lessons), on the understanding that you agree to follow these guidelines. These guidelines apply to all staff and pupils.

You should be aware of the following:

1. Computer (file) storage areas are school property.

2. All network activity is monitored and recorded.

3. All emails (even when deleted) and their history are logged and archived.

4. ICT staff use network monitoring and alerting systems to provide remote support and to ensure the school systems are being used in accordance with the school's rules

5. Members of the ICT staff may look at any files and communications to insure that the system is being used responsibly

6. ICT staff can view any school computer screen at any time from anywhere on the school network without you knowing about it.

The following are not permitted:

- Use of another person’s username and associated password.

- Trespass in others' folders, work or files.

- Hacking or hacking with intent to cause damage.

- Downloading viruses, trojans or circulating “infected files”.

- In any way enabling yourself or others to gain unauthorised access to computer material (this includes instructions for gaining such access, computer codes or other devices which facilitate unauthorised access);

- Allowing another person to use your username and password.

- Sending, displaying, accessing or trying to access any obscene, offensive or hate crime material.

- Using obscene or offensive language.

- Harassing, insulting or attacking others through electronic media including on grounds of age, gender, race, disability.

- Unauthorised copying of software or violating copyright laws.

- Revealing any personal information, the home address or personal phone numbers of yourself or other people to anyone, unless specifically authorised by parent, carer or teacher.

- Downloading games or other executable programs.

- Intentionally wasting limited resources or time on unnecessary or unauthorised activities.

- Moving or changing any computer or associated equipment unless specifically requested and authorised by a member of ICT staff. Damage caused by unauthorised persons may be considered a criminal offence.

- Eating, drinking, using aerosols etc near any electronic equipment.

- Use of commercial activities by for-profit institutions.

- Carrying on a private business.

- Undertaking financial transactions on behalf of the school unless authorised.

Additional Information

- The School’s wired and wireless networks, Internet access and school email are provided for users to conduct genuine research and communicate with others. All your activity and the sites you visit are recorded. Remember that access is a privilege, not a right, and that access requires responsibility at all times.

- During lessons, teachers will guide pupils toward appropriate materials. Outside of lessons, families and / or carers bear responsibility for such guidance, as they do with other information sources such as television, telephone, cinema, radio, newspaper, magazine and other potentially offensive media.

- All users are required to log on using only their own personal username, which will remain with them throughout their time at the school. Use of another person’s username and password is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed in the appendices.

- Trespass in others' folders, work or files. All unauthorised access is considered a criminal offence under the Computer Misuse Act 1990 and/or depending on offence any other Act listed in the appendices.

- Users' passwords must not be made available to anyone else. If you think someone has learned your password then change it immediately. Change your password at regular intervals; at least once a term and using a minimum of twelve (12) characters, including numbers and letters. Do not write your password on anything you leave unattended.

- Remember a school is a public place. Always make sure that you have completely logged off or locked the computer before leaving it unattended. Failure to do so will be considered a contravention of school policy and if an offence has been committed by some other person, may be considered as facilitating the Misuse of Computer, which is also a criminal offence

- Damage to data, computers, computer systems or computer networks, including unauthorised damage or interference to any files or program is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.

- Programs must not be installed on a computer except by a member of the ICT administration department.

- The installing, copying or transmitting of obscene material is not permitted and may be considered a criminal offence under the Obscene Publications Act 1959/1964.

- If a "virus alert" occurs when transferring work files from anywhere, please inform your teacher and a member of the ICT staff immediately.

- Computer equipment may not be taken off-site without formal authorisation.

- During the day when not in use, computer screens should be switched off to save electricity however the computers should be left logged off but powered up. Computers will be shutd own by the ICT systems at the end of the day after maintenance.

## Sanctions

Remember that the use of the School's IT facilities in a way which contravenes the School's regulations may be treated as a disciplinary offence and lead to the penalties established by those regulations.

1. Violations of the above rules will result in a temporary or permanent ban on your use of the school network.

2. Additional disciplinary action may be added in line with existing practice on inappropriate language or behaviour including detentions, formal warnings, informing of parents and noted on school records.

3. When applicable, police or local authorities may be involved.

## File Storage and Security

- The school uses Google GSuite for Education for email, file storage and other applications. Google Drive provides unlimited drive space in the cloud for each school user while they are a member of the school. All staff and students are directed to save their work on their Google Drive as their main storage area.

- Additionally all users have a limited own area for storing some of their work on the school's network servers (usually designated the "H" drive) when using applications installed on school machines. This means that they can access their work from any school network station.

- To reduce the chances of the server hard disks filling up and crashing the whole network, the amount of disk space for each user is limited to normally 500MB. Overflowing this limit will cause the user to be locked out until sufficient files have been deleted or uploaded to their Google Drive.

- Users are not permitted to use memory sticks; users must go to the ICT administrators' office to request the archiving of files to memory sticks, if required.

- Users are not permitted access to station and network drives other than those provided at login; nor are they permitted to alter or save files outside their own area (except in the authorized shared areas).

- Network stations may not be booted up from USB or CD. Unauthorised users (anyone excluding ICT administration staff) attempting to do so will be in breach of the Computer Misuse Act

- An automatic regular search will be made for any executable program and zip files stored in user areas. These will be noted, automatically logged against the user and the user notified. If the user cannot provide a satisfactory reason for them, the authorities will be notified and appropriate action will be taken.

## Access to Software

- At logon all users receive desktop icons and start-menu-shortcuts to all the main application programs and common utilities, on the wired network, set up for each of the curriculum subjects. This provides shortcuts/icons to programs that are relevant to the study of that subject as well as any shared documents provided by the subject teachers. Pupils have read-only access to these shared documents but may copy them for their own use. Attempts to modify these are in breach of the Computer Misuse Act

- Users may only access software and other resources as made available to them through these subject shortcuts. For example, pupils do not have access to the Staff areas. Access to certain resources such as Internet software may also be removed for certain network users, where found to be necessary.

- Use of the main applications software is continually audited for each user. Sites visited on the Internet are also audited, and filtered by our Internet Service provider and our own filtering and monitoring appliances.

- Attempts to access sites blocked by the ISP or school are in breach of the school policy. Where a site is blocked and is required for school work, the ICT staff may be requested to ask for the site to be unblocked by a member of staff.

### Access to Printers

- To encourage good management and reduce wastage of ink and paper, the number of print credits for each user is currently limited to an annual limit of £10.00 in years 7,8 and 9; £15.00 in years 10 and 11 and £20.00 in years 12 and 13.

- Attempts to print beyond this credit limit are automatically denied by the system. Pupils may purchase more credits from the finance office. The cost of these is 1p per credit with a minimum purchase of £1. Please Note: Currently 5 credits are used for a black print A4 page and 20 credits are used per page for expensive printers and for colour printing.

**Your Input**

We welcome your input in respect of suggesting material which should be filtered or unfiltered, although Sir William Borlase’s Grammar School maintain the right to ultimately determine what is and is not filtered.

**Appendices**

**Computer Misuse Act 1990**

The "Computer Misuse Act 1990" covers three offences

- Simple hacking, that is the unauthorised entry to computer facilities via a computer.

- Unauthorised access with criminal intent, that is hacking with the intention of perpetrating a more serious crime and covers facilitating access to others.

- Unauthorised amendment or damage to data and covers among other things the introduction of viruses and time bombs.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 5 years.

Anyone suspecting that an offence has been committed should refer the matter to the Headteacher.

**Data Protection 1998 and (Charges and Regulations) 2018 - GDPR**

The General Data Protection Regulations (2018) concerns the processing of information about living individuals. It gives rights to those individuals about whom information is recorded and demands good practice in handling information about people.

You must:

- only use personal data for a School related purpose;

- ensure that the use of School related personal data is restricted to the minimum consistent with the achievement of academic purposes;

- contact the School's Business manager or Data Protection Officer before conducting any activity which involves the collection, storage or display of personal data through the School's IT facilities.

Any use of personal data beyond the descriptions listed in School's registration is illegal.

**Malicious Communications Act 1998**

Under Section 1 of this Act it is an offence to send an indecent, offensive or threatening letter, electronic communication or other article to another person.

**The Telecommunications Act 1984**

It is a similar offence to send 'by means of a public telecommunications system, a message or other matter that is grossly offensive or of an indecent, obscene or menacing character' and is an imprisonable offence with a maximum term of six months and/or a fine up to £5000.

**Protection from Harassment Act 1997**

Stalking, Offensive or threatening communications can also be charged under the Protection from Harassment Act. This can carry a sentence up to 5 years imprisonment.

**Sex Discrimination Act 1975**

Discrimination on the grounds of sex by dismissing an employee or submitting them to "any other detriment"

**Race Relations Act 1976**

As above, but on racial grounds

**Disability Discrimination Act 1995**

As above, but on grounds of disability

**Criminal Justice & Public Order Act 1994**

Intentional harassment for causing another person harassment, alarm or distress by using threatening, abusive or insulting words or behaviour

**Obscene Publications Act 1959 and 1964**

It is an offence to publish an obscene article or to have an obscene article in ownership, possession or control with a view to publishing it or, where the data is stored electronically, to transmit that data.

**Copyright, Designs & Patents Act 1988**

The "Copyright, Designs & Patents Act 1988" provides the same rights to authors of computer programs as literary, dramatic and musical authors have to their works. Those rights extend for the life of the author and for fifty years after the author's death.

Software is generally not sold outright to the purchaser. Instead the purchaser is granted the right to use it as laid down in the user licence. It is normally expected that only one person at a time will have access to and use the software concerned. A network licence may be purchased, normally at a reduced rate, for a defined number of users. A site licence may be available to cover all (unlimited) users within the premises.

It is thus illegal to make copies of software without the copyright owner's consent, or to duplicate software loaded on a hard disk for use on any other personal computer unless allowed for under the licence.

Anyone convicted of an offence under this act can expect a fine of unlimited amount plus a prison sentence ranging up to a maximum of 2 years.