Coláiste Bhaile an Droichid

Bridgetown College

Baile an Droichid Co Loch Garman
Bridgetown Co Wexford
Y35 R628

wwetb

Bord Oideachais agus Oiliúna
Phort Láirge agus Loch Garman
Waterford and Wexford
Education and Training Board

Acceptable Usage Policy

INFORMATION AND COMMUNICATIONS TECHNOLOGY USE

Ratified by the Board of Management: 9 May 2017

T: (053) 9135257 email: bridgetowncollege@wwetb.ie Uimhir Rolla/Roll No: 71610E

Table of Contents

Aims of the Acceptable Usage Policy

The aim of this Acceptable Use Policy is to ensure that Students will benefit from learning opportunities offered by the school's internet resources in a safe and effective manner. Internet use and access is considered a school resource and privilege. Therefore, if the school's AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions – as outlined in the AUP – will be imposed.

It is envisaged that school will revise the AUP annually or as the need arises. Before signing, the AUP should be read carefully to ensure that the conditions of use are accepted and understood. This version of the AUP was updated on the 20 December 2016.

Background

Bridgetown College has three computer rooms, each with 24 workstations plus one connected to a data projector for the teacher. The rules for the computer rooms are outlined in Appendix 1. Students who do not follow these rules will be liable to sanctions outlined below. It is the teacher's responsibility to make sure all the computers are in working order when they enter the room and when they leave the room. A report is provided in this document that is available in all of the computer rooms. [Appendix 2]. On this sheet is also a facility for reporting any problems with any of the computers in the rooms. All teachers using the computer room should have a seating plan and be able to identify which terminal particular students were sitting at. A timetable is put up in each room each week and teachers may book the room if there is a free space. Use of the computer room should always be pre-planned.

Every classroom in the College now has its own computer and data projector. This is to facilitate the use of IT as a teaching and learning tool and also to facilitate the use of a Student Management System for the calling of rolls and registers and other functions as set out below. Teachers must ensure that students should not have access to these computers unless they are strictly monitored and never in the absence of a teacher. On enrolment, parents must give permission for an account to be set up for their son/daughter and for them to use the school's IT facilities. [Appendix 3] Failure to agree to this will exclude the student from and IT related activities.

The school Computer System

Office 365 for Education

This is a collection of services that allows teachers and students to collaborate and share schoolwork. Every staff member and student in the school has their own Office365 account. This allows for 1TB of cloud storage, access to the office programs online, school E-mail and the facility to download the full version of the latest Microsoft office products onto up to five personal devices.

Each student is assigned an Office 365 account accessed using a school email address and password. The E-mail address is in the format YYFirstnameLastname@bridgetownvoc.ie. It is

envisaged that this account will be used by students when engaging in school work or collaborating with teachers/students in the course of school work. As this account can be accessed through a web browser, students will have access both in school and at home. The school does not accept responsibility for students' use of Office 365 outside of school time.

- Pupils are responsible for having their login details available during school hours
- Pupils should report any account issues – locked out, no access…to their class teacher.
- Parents are requested to monitor the student's use of the account outside of school

Cloud Storage

This facility is designed to allow teachers/students to store school related work/projects, making it accessible to use from home or elsewhere.

- Pupils should only upload course-related documents/work.
- Pupils should not allow anyone else to access their OneDrive.
- Pupils are not permitted to access or modify another student's OneDrive
- Pupils should not reveal their password to anyone

The responsibility for what is stored and uploaded to OneDrive lies with the students and parents.

Student Accounts: These are set up for each student in first year. These accounts stay with the students until they leave the College. All students have their own log in and password that gives them access to these accounts. Their login details for the computer system are the same as those for logging in to Office 365 (See Below). No other student has access to any other student's material. It is the responsibility of each student to ensure that their password is kept secret. Student passwords are generated by VSware. Should a student change their password it will reset to the original the next time VSware is synchronised with Office 365. Therefore, students should not change their passwords. If they feel that their password may have been compromised, only VSware system administrators can reset them. These include the Principal, Deputy Principal and office admin staff. IT support of WWETB can also reset passwords at any time.

Student Shared Account:

VSware is responsible for setting up groups within Office365 so that each teacher has access to their teaching group as does each student within that group. A suitable use for this might be for a teacher to upload documents or resources to it for all their students to use. Students may not use this shared space to post personal messages of any sort or interfere with any material uploaded to it that is not theirs.

Staff Accounts:

Every staff member has their own computer account that only they and the ETB IT administrator will have access to. The staff accounts are logged into as follows.

Username [teacherfullname]. Password[Office365 Password]

School Strategy

The school will employ a number of strategies in order to maximise learning opportunities and reduce risks associated with the Internet. These strategies are as follows:

General

- Internet sessions will always be supervised by a teacher.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material.
- The school will regularly monitor students' internet usage.
- Teachers will be provided with training in the area of internet safety.
- Uploading and downloading of non-approved software will not be permitted.
- Virus protection software will be used and updated on a regular basis.
- The use of personal removable storage devices in school requires a teacher's permission.
- Students will observe good "netiquette" (i.e., etiquette on the internet) at all times and will not undertake any actions that may bring the school into disrepute.

Browsing Websites

- Students will not visit Internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will use the internet for educational purposes only.
- Students will be familiar with copyright issues related to online learning.
- Students will never disclose or publicise personal information.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored for unusual activity, security and/or network management reasons.

Email

- Students will use approved school email accounts. As students have access to these E-mail accounts outside of school, they are responsible for ensuring that they use these E-mail accounts within the limits of this Acceptable usage policy set out below;
  - Students will not send or receive any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
  - Students will not reveal their own or other people's personal details; such as addresses or telephone numbers or pictures.
  - Students will never arrange a face-to-face meeting with someone they only know through emails or the internet.
  - Students will note that sending and receiving email attachments is subject to permission from their teacher.

Internet Chat / Social Networking

- Students will only have access to chat rooms, discussion forums or other electronic communication forums that have been approve by the school.
- Chat rooms, discussion forums and other electronic communication forums will only be used for educational purposes and will always be supervised.
- Usernames will be used to avoid disclosure of identity.
- Students will not access social networks.
- Students will not post defamatory remarks about the school or set up unauthorised social networking sites in the name of the school.

School Website

- Students may be given the opportunity to publish projects, artwork or school work on the Schools website.
- The publication of student work will be co-ordinated by a teacher.
- Students' work will appear in an educational context on Web pages with a copyright notice prohibiting the copying of such work without express written permission.
- Digital photographs, audio and video clips will focus on group activities. Video clips may be password protected.
- Personal Student information including home address and contact details will be omitted from school web pages.
- Students will continue to own the copyright on any work published.

Printing

- There are a number of printers placed around the school. All of the printer drivers download to the teacher's profile on first login. Each computer room has a Mono printer. There is a colour printer in the teacher's workroom and the storeroom across from the Staffroom. These printers are set to default to black & white. To print in colour staff must select it in the printer settings.
- Students do not have access to any of the printers in the school.
- Students wishing to print must share the documents they wish to print with their teacher.
- Staff should print to the printer in that computer room unless it is not operational or unless they need to print colour. To this end, printing should be done in black and white where possible to minimise the cost to the school.
- Paper will be recycled where possible to minimise cost to the school and minimise environmental impact.
- Any problems with printers including running out of ink should be reported immediately to the office where our print management provider will be contacted.

School MIS (VSware)

VSware is our current School Management System. It is used exclusively by staff members within the school network. Staff can access VSware from outside the school network as it is cloud based. For this reason, it is important that school Staff follow the following guidelines.

- Staff must protect the integrity of the student data at all times, both inside and outside of school.
- The Student Management System must never be left open and unsupervised.
- Staff must ensure that their passwords are not written down or accessible to anyone.
- Staff must ensure that their passwords are sufficiently strong to ensure that they cannot be easily guessed or hacked. Best practice suggests that passwords should be at least 8 characters long and consist of three of the following. Capital letters, regular letters, numbers and symbols. Our Student Management System is set up to insist that this protocol is followed.
- In general, students or parents do not have access to VSware at present. However, for the purposes of entering LC1 subject preferences, parents of current 3rd year and Transition Year students are given access.

Legislation

The school will provide information on the following legislation relating to use of the Internet which teachers, students and parents should familiarise themselves with:

- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1998
- Interception Act 1993
- Video Recordings Act 1989
- The Data Protection Act 1988

Support Structures

The school will inform students and parents of key support structures and organisations that deal with illegal material or harmful use of the Internet.

A secure Environment
- When not in use the doors to the computer rooms must be kept locked.
- Knowledge of passwords or loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from others users, gain unauthorised access to resources or otherwise make use of computing resources for which proper authorisation has not been given.
- Users are responsible for the proper saving or their material in the appropriate place in their account on Office 365. It is not necessary for students to bring external memory devices to school as Office 365 is backed up on a regular basis.

Support Policies
- The following overarching WWETB policies must be adhered to and can be located by following the links below;

     o Acceptable Internet Usage Policy;

http://waterfordwexford.etb.ie/wp-content/uploads/sites/24/2014/12/Acceptable-Internet-Use-Policy-March-2014.pdf

     o Acceptable E-mail use Policy

http://waterfordwexford.etb.ie/wp-content/uploads/sites/24/2014/12/Acceptable-Email-Use-Policy-March-2014.pdf

     o Computer Password Policy

http://waterfordwexford.etb.ie/wp-content/uploads/sites/24/2014/12/Computer-Password-Policy-March-2014.pdf

     o Mobile Computer Use Policy

http://waterfordwexford.etb.ie/wp-content/uploads/sites/24/2014/12/Mobile-Computer-Use-Policy-March-2014.pdf

     o Wireless Use Policy

http://waterfordwexford.etb.ie/wp-content/uploads/sites/24/2014/12/Wireless-Use-Policy-March-2014.pdf

Sanctions

Misuse of the Internet may result in disciplinary action, including written warnings, withdrawal of access privileges and, in extreme cases, suspension or expulsion. The school also reserves the right to report any illegal activities to the appropriate authorities.

Parents may be asked to furnish the school with the IP address of any home internet account that is used in a malicious or offensive manner regarding communications to or from the school. The IP address will be used in order to establish beyond reasonable doubt the origin of said malicious or offensive material.

Teacher access to the computer rooms

There are 2 different types of classroom usage:

First: Timetabled IT classes: - Regular IT classes which have been timetabled for the use of specific IT rooms to meet their needs.

Second: Any other type of class which requires the occasional or once off use of an IT room may book the room in advance which helps ensure fair usage for all teachers and classes. The booking sheet will be in the staffroom.

In the event that specific software or hardware is not available, the school IT administrator will present a proposal to the principal for the purchase of said software or hardware.

In the event of damage caused to IT equipment, the teacher of the class must fill out a damage report and file it with IT administration. If such damage is found to be malicious, the student

involved will be reported to his Year Head and monies sought from their parents to pay for the damage.

School IT Administrator

The school IT administrator has a number of key roles;

- To deal with any minor issues that may arise that can be easily fixed at a local level.
- To order IT supplies as needed.
- To liaise with school administration in relation to student passwords.
- To communicate to head office any new students or staff that need to be set up with both school accounts and Office 365 accounts.
- To report serious problems to the ETB IT department as soon as they may arise.
- To liaise with ETB IT department staff once a week onsite to discuss maintenance / repair works that need to be carried out.

The IT administrator in the first instance is WWETB. The local school IT administrator is a teacher with a post of responsibility where possible.

The current school IT Administrator is _____.

This version of the Acceptable Usage Policy was created on 9 May 2017

and was ratified by the Board of Management of Bridgetown College on 9 May 2017

Signed:

_____

(Chairperson)

Appendix 1

Rules for the Computer Room

1. No food or drink in the Computer Room.

2. Do not interfere with any of the computers or equipment.

3. If the computer is not working properly. Do not attempt to fix it yourself. Call your teacher.

4. Do not access unauthorised material on the internet.

5. If you inadvertently access material you know you should not't while using the internet, alert your teacher immediately.

6. If you wish to use a memory stick from home, get permission for your teacher first.

7. You do not have permission to install any software on the school computers.

8. At the end of each class, shut down the computer. Turn off the monitor also to save electricity.

9. At the end of the class, pick up any litter at your workstation. Ensure you push in your chair.

Appendix 2

Computer not working report for teachers using IT rooms

Date: _____   Time: _____

Computer (4th on left etc): _____

Details   Problem:

_____
_____
_____
_____

Did the problem arise during the course of the class or was it there when you entered?

_____
_____
_____
_____
_____

Any other observations?

_____
_____
_____
_____
_____

Signed Class Teacher: _____   Date: _____

Appendix 3

Permission to use the computer equipment

The following section is included in out enrolment form and if no permission is given then that particular student cannot use the school's IT equipment. Parents should understand that this could compromise some of their examination grades at state level due to the research component of some of the project work.

<u>Pupil Computer Account Agreement</u>

The college's Acceptable Usage Policy is currently under review. It outlines the rules and regulations governing the use of the school's computers and computer systems. All students in the school are offered their own computer account and an Office 365 account which gives them access to their own storage space on the school server as well as internet access.

Please tick one of the boxes below to indicate whether you give permission for your son/daughter to have his/her own computer account on the school server in addition to an Office 365 account.

I give permission.	☐
I do not give permission.	☐

Please tick to indicate your preference.