CBS Secondary School, Dungarvan.

Information Technology (IT)

Acceptable Use Agreement Policy

POLICY STATEMENT:

Dungarvan CBS Secondary School is committed to ensure that all users including students, staff and parents will benefit from learning opportunities offered by the school's Information Technology (IT) system in a safe, effective and appropriate manner.

The Aims of This Policy:

- To promote the professional, ethical, lawful and productive use of Dungarvan CBS's IT systems
- To define and prohibit unacceptable use of Dungarvan CBS's IT systems
- To educate users about their IT Security responsibilities
- To promote practices to ensure appropriate confidentiality and non-disclosure of the School's sensitive information
- To describe where, when and why monitoring may take place

If the school's **IT ACCEPTABLE USE POLICY** is not adhered to, access to the school's IT system may be withdrawn and appropriate disciplinary actions will be imposed in accordance with established procedures.

This document is divided into 3 sections

Section 1: Applies to all - students, staff, volunteers and parents who access IT.

Section 2: Applies to Staff Only

Section 3: Applies to Students Only

Section 1 - Applies to All

- General Principles
- Desktop Computers
- Email
- Your Password
- Web access and content filtering
- Social Media and Cyber-Bullying
- Responsible use of resources
- Monitoring

Section 2 - Applies to Staff Only

- Laptops
- Data Protection
- Printing
- Disciplinary actions

Section 3 - Applies to Students Only

- Laptops
- Printing
- Disciplinary actions
- Acceptance

Section 1 – Applies to All

General Principles

Things to know

- Information Security is everybody's responsibility.
- The school's IT systems are provided for educational use.
- Use of any of the school's IT systems for personal reasons (including e-mail and the web) is only permitted in accordance with the guidance in this policy.
- The school reserves the right to monitor any aspect of its information systems in order to protect its lawful interests, prevent and/or detect crime, discriminatory and harassing behaviour. Information gathered from such monitoring may be used to instigate or support disciplinary proceedings and may be disclosed to the Gardaí or any other investigatory body.
- This policy refers in several places to things that "Others may find offensive". These include but are not limited to:-
    - Pornographic or sexually explicit material
    - Discriminatory and harassing behaviour
    - Tasteless material (such as depiction of injury or animal cruelty)
- The school will deal with incidents that take place outside the school that impact on the wellbeing of students or staff under this policy and associated policies. In such cases the school will, where known, inform parents/carers of incidents of inappropriate online behaviour that take place out of school and impose the appropriate sanctions.

- The school implements the following strategies on promoting safer use of the internet:
    - Education for students in internet safety as part of the Wellbeing curriculum.
    - The school participates in Safer Internet Day activities
    - Teachers will be provided with CPD opportunities in the area of internet safety.
    - Internet safety advice and support are provided to students through our First Year Induction day, computer classes & pastoral care.
- Should serious online safety incidents take place, the Designated Liaison Person (DLP) for child protection, the Principal, should be informed.

Things to do

- Treat others with respect at all times.
- Respect the right to privacy of all members of the school community.
- Respect copyright and acknowledge creators when using online content and resources.
- Exercise care and common sense in your use of information technology.

Things not to do

- Anything illegal.
- Anything that contravenes this policy.
- Anything that will harm the reputation of the School.
- Anything that contravenes the School's Dignity in the Workplace, Code of Behaviour and Antibullying Policies.

Desktop Computers

Things to know

- Desktop computers are the property of the school and have been prepared by the IT department for use on the school network.
- Authorised software is installed on your computer and you are not allowed to install anything on your own.
- Data saved to local drives will not be backed up, and will be lost if the computer breaks, gets stolen or is replaced. Therefore, it is highly recommended and it is your responsibility to store all your data securely.
- The school may at any time and without prior notice:-
    - Audit the computers to ensure compliance with policy.

Things to do

- Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.
- Ensure that files received from anywhere outside the school are virus checked before you open them.
- If you suspect a computer you are using may have a virus, leave the computer on, unplug the network cable and call the IT Co-ordinator.
- Turn any PC and monitor off at night to save energy unless there is a specific reason to leave it on.

Things not to do

- Do not allow anyone else to use a computer while you are logged in.
- Never install software on your computer. This should only be done by the IT Technician. Things that you should never attempt to install include but are not limited to:-
    - Screen savers and games, music download software.
    - Utilities that claim to remove spyware or viruses.
    - News readers or ticker-tape services.
    - Applications that download torrents such a showbox, popcorn, moviebox etc
- Do not disable or uninstall any of the software that is installed on your computer.

Email - Office 365

Things to know

- The school's e-mail systems are provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.
- The school reserves the right to monitor all e-mail to ensure compliance with policy
- E-mail is not a secure method of communication. Once a message is sent you have no further control over who reads it.
- E-mail is admissible evidence in any legal proceedings and carries the same weight as a letter on school headed paper.
- School email accounts may not be used to register for online services such as social networking services, games and purchasing.
- Students will use approved email accounts only under supervision by or permission from a teacher.

Things to do

- Use the same care when drafting an e-mail message as you would when writing a letter or memo on school headed paper.
- Make sure that your message is concise, relevant and sent only to the people that need to read it.
- Check your e-mails every day and clear out old and unwanted messages from your mailbox.
- Return any wrongly delivered message to the sender. If it contains confidential information it should not be disclosed or used in any way.
- Immediately report to the principal the receipt of any communication that makes you feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and do not respond to any such communication.

Things not to do

- Never open an attachment that you were not expecting, even if you know the sender.
- Do not use personal emails accounts for any school communication or business.
- Do not use e-mail to send sensitive or confidential information.
- Do not send or forward anything that:-
    - Is illegal, obscene, others may find offensive, may be defamatory or harassing
    - Is covered by a copyright (pictures, movies, music, others)

- Do not circulate non school-related material. This includes but is not limited to:-
    - Chain letters, jokes, virus warnings, software
- Never use e-mail to rebuke, criticise or complain about somebody. You may say something that you regret, and the record will be permanent.
- Never supply banking or payment details in response to an e-mail message. This is a well-known method of fraud. Your bank will never request security details by e-mail.

Your Password

Things to know

- Your password is confidential and it is not transferable to anyone else.
- The password requirements for Office 365 must be at least 8 characters long and contain a capital, a lowercase and a number.
- You can change your password at any time (from the CRTL + ALT + DEL menu), not just when the system prompts you.
- The access rights associated with your Office 365 account may be changed or revoked should your status as an employee or student change/terminate.

Things to do

- Set a password or phrase. Make it as secure as you can by using some or all of the following techniques:-
    - Use two unrelated words or a short phrase.
    - Include at least one number.
    - Include at least one upper case character.
    - User name can't be part of your password.
    - Password has to be at least 8 characters long.
- Change your password if you suspect that someone else may know it.

Things not to do

- Do not use one of the 'top 6 predictable passwords':-
    - Your birth date or birth date of one of your relatives.
    - The name of a family member.
    - The name of a pet.
    - Your football team.
    - A rude word.
    - An item or brand name that you can see from your desk.
- In general do not use for your password anything that can be easily associated with you
- Do not disclose your password to anyone.
- Do not use anyone else's password.
- Do not write down your password. You need to remember it.

Web Access and Content Filtering

Things to know

- Web access is provided for school use. Reasonable personal use is permitted provided it is lawful, ethical and takes place during authorised breaks.
- The school has chosen to implement level 4 content filtering on the schools broadband network, which aligns to NCTE guidelines:
    - This level allows access to millions of websites including games and You Tube but blocks access to blogs and social networking sites like Facebook. This content filtering applies to school devices and personal devices.
- Any person taking steps to by-pass the content filter by any means may be subject to disciplinary action.
- All web access can be monitored by the school to ensure compliance with the policy. Users that choose to make personal use of the school's IT system do so in acceptance of the monitoring measures outlined in this policy.

Things to do

- Use the school's internet connection for educational and career development activities only.
- Report accidental accessing of inappropriate materials to the teacher or IT Co-ordinator.
- Sites that are blocked usually ask you to click on a particular section to fill in a request to have the site reviewed by the NCTE as appropriate for teaching purposes. Please use this method of getting sites unblocked as the IT Co-ordinator has no control over unblocking sites.
- If you suspect a computer you are using may have a virus or spy-ware infection, leave the computer on, unplug the network cable and call the IT Co-ordinator.

Things not to do

- Do not view or download anything that others may find offensive, illegal, obscene and defamatory. This includes, but is not limited to:-
    - Pornography, Racism, Terrorist sites
- Do not upload or download large files that results in heavy network traffic and affect performance for other users.
- Do not download anything that is likely to be covered by copyright. This includes, but is not limited to:-
    - Music, Pictures, Software and Movies
- Do not visit the "high-risk" site categories shown below. Although their content appears to be free, it is often funded by installing spyware on your computer.
    - Free screensavers and smileys
    - Free music downloads or ring tones
    - Free software and serial numbers (also known as cracks)
    - Adult material
    - Films from streaming sites (moviebox)
- Do not download any attachments using personal web based mailboxes (Yahoo, Hotmail etc.) as it is not monitored by the school security software.
- Do not listen to the radio stations through internet as the radio stream consumes too many resources in the network that will affect performance.

Social Media and Cyberbullying

Things to know

- The use of instant messaging services and apps including Snapchat, WhatsApp, GChat etc. is strictly prohibited on the School network.
- The use of Blogs such as Word Press, Tumblr, etc. is allowed with express permission from teaching staff.
- The use of video sites such as YouTube and Vimeo etc is allowed with express permission from the teaching staff.
- Engaging in online activities with the intention to harm, harass, or embarrass another student or member of staff is an unacceptable and absolutely prohibited behaviour, with serious consequences and sanctions for those involved.
- Measures are taken within the School to ensure that staff and students are aware that bullying is defined as unwanted negative behaviour - verbal, psychological or physical - conducted by an individual or group against another person (or persons) and which is repeated over time. This definition includes cyberbullying even when it happens outside the school or at night.
- Isolated or once-off incidents of intentional negative behaviour, including a once-off offensive or hurtful text message or private messaging, do not fall within the definition of bullying and will be dealt with, as appropriate, in accordance with the school's code of behaviour.

Things to do

- Use Blogs in a safe and respectful manner.
- Use blogs for educational purposes.
- Treat others with respect at all times.
- Report any incident of cyber bullying to the Deputy Principal.

Things not to do

- Do not use social media in any way to harass, insult, abuse or defame students, their family members, staff and other members of the school community.
- Do not discuss personal information about students, staff and other members of the school community on social media.
- Do not represent your personal views as those of being CBS Secondary School's on any social medium.

Responsible Use of Resources

Things to know

- Implementing the small changes described on this page can make a big difference to the school's costs, and also to the environment.
- Phone chargers and AC adapters consume a small amount of power even when nothing is connected to them.

Things to do

- Shut your computer down at the end of your working day rather than just logging off. The energy saved over a year is enough to boil 60 tonnes of water.
- Turn off your monitor before you leave rather than leaving it in standby (1.5 tonnes).
- Unplug or switch off phone, PDA or portable device chargers when they are not in use.

Things not to do

- Do not turn off computer equipment on behalf of someone else. There may be a good reason why it has been left on.

Monitoring

The school owns its IT systems. It reserves the right to monitor any school system at any time. Monitoring of any device/system can be done by or on request from the Principal, Deputy Principal, IT Technician associated with the school. Monitoring of systems is carried out by the Principal and IT Technician in order to:-

- Detect and prevent unlawful use of systems.
- Detect and prevent misuse of school systems.
- Maintain the effective operation of systems.
- Protect the School's employees.
- Protect the reputation of the school.
- Protect the School from legal liability.

Monitoring of systems will be conducted in accordance with the provisions of legislation in force from time to time, in particular:-

- General Data Protection Regulation (GDPR) May 2018
- Data Protection Act 1998
- Data Protection (Amendment) Act 2003
- Child Trafficking and Pornography Act 1997
- Interception Act 1993
- Video Recordings Act 1989
- Human Rights Act 1998 and the European Convention on Human Rights (if applicable)

At the request of the Board of Management or as needed, management of the school may pass on requested data to any of the following:

- The Principal
- The Gardaí
- Other parties as required by law

Section 2 – Applies to Staff Only

Laptops Insurance

- Teacher Laptops are school property and are, therefore, insured under the school insurance contents policy.
- Laptops are insured if damaged or stolen when on-site or off-site. This covers being out and about on school business, school tours or theft from a staff member's home.
- If a device is being transported in a car it must be kept in the boot, out of sight at all times and the car must be locked.

Things to know

- Laptops are the property of the school and have been prepared by the IT Technician for use on the school network.
- If your contract has ceased with the school, you have retired, are on Maternity Leave or Career break the Laptop must be returned to the school before you leave.
- Authorised software is installed on your computer and you are not allowed to install anything on your own. Please talk to the IT Technician if you would like to download anything else.
- Data saved to local drives will not be backed up and will be lost if the computer breaks, gets stolen or is replaced, therefore, it is highly recommended and it is your responsibility to store all your data.
- The school may at any time and without prior notice:-
    - Audit the computers to ensure compliance with policy.
- You are taking full responsibility for everything done on your portable computer.
- You are responsible for the care and safe storage of any computer equipment that has been issued to you.

Things to do

- Return your device if you are no longer working at Dungarvan CBS for a considerable amount of time.
- Always consider the physical security of your portable computer:-
    - In an unlocked office - Kept in a locked drawer.
    - In the car - Do not leave your portable device in the car.
    - While in transit - stored in the boot of the car.
    - At home - Ideally within a locked work area. Otherwise, within a locked drawer
    - In a hotel - Concealed from view. Ideally locked in a suitcase or safe.
    - Travelling - Keep the computer on your person and out of sight at all times.

Things not to do

- Never install software on your computer. This should only be done by the IT Technician. Things that you should never attempt to install include but are not limited to:
    - Screen savers and games, music download software
    - Utilities that claim to remove spyware or viruses or News readers or ticker-tape services.
    - Applications that download torrents such a showbox, popcorn, moviebox, etc.

- Do not allow family, friends or anybody else to use the computer.
- Do not leave portable computers on view within a car. Always keep them in the boot.
- Be conscious of the risks while you connect your portable device to a non-office network (hotel, airport) always use a VPN to get access to the internet or school data.
- Do not allow visitors (guest speakers, etc.) to connect their laptops to the school's network before getting the approval from the IT Technician.

Data Protection Responsibilities

Things to know

- You are personally responsible for ensuring the confidentiality of a student's personal data.
- Student information is now accessible on VSware which is password protected.
- If student information is put onto a USB, the files on the USB must be encrypted.

Things to do

- Log off from any workstation (CTRL+ALT+DEL) once you are finished using it.
- Ensure Anti-virus programme is running on your Laptop.
- If Personal Data is saved to a USB drive ensure it is fully encrypted.
- If you process personal data (data that identifies a living individual) in the course of your work, you must do this in accordance with General Data Protection Regulation (GDPR) May 2018.

Things not to do

- Do not view sensitive information on the train, plane or in any public area. This provides an opportunity for onlookers.
- Do not allow family, friends or anybody else to use the computer which contain student information.
- Do not disclose or share any sensitive information to other people if not under the expressed authorisation of the Principal.
- Do not leave printed documents around the printer as they may contain confidential data.

Printing

Things to know

- Printers are provided for education use only.

Things to do

- Be selective about what you print. Print only when necessary and only the necessary pages of a document.
- Use a photocopier when producing a large number of copies.
- Keep the area around printers tidy.

Things not to do

- Do not resend your print job if nothing happens. Instead, check the following:-
  - Is the print job still listed in the queue?
  - Is the printer switched on?
  - Is the printer in an error state because:- (a) There is paper jam (b) It is out of paper (c) It is out of toner or ink.
    If any of those occurs please contact Reception.
  - Mindless printing is an offence to carbon footprint.
  - Do not leave printed documents around the printer as they may contain confidential data.

Disciplinary Action for Staff

Breach of this policy may lead to the implementation of disciplinary procedures as set out by the Teaching Council and DES. This process is described as follows:

1. Verbal warning
2. Written warning.
3. Serious or persistent breaches may constitute gross misconduct and disciplinary procedures laid out by the Teaching Council and Department of Education and Skills will be followed.

Section 3 – Applies to Students Only

Printing

Things to know

- Printers are provided for education use only and supervised by teaching staff.

Things to do

- Be selective about what you print. Print only when necessary and only the necessary pages of a document.

Things not to do

- Do not resend your print job if nothing happens. Instead, check the following:-
    - Is the print job still listed in the queue?
    - Is the printer switched on?
    - Is the printer in an error state because:- (a) There is paper jam (b) It is out of paper (c) It is out of toner or ink o If any of those occurs please contact reception.
- Mindless printing is an offence to carbon footprint

Disciplinary Action for Students

Breach of this policy may lead to the implementation of the school's Code of Behaviour.
This process is summarised as follows:

1. Verbal warning.
2. Written warning.
3. Withdrawal of access privileges.
4. Detention.
5. In extreme cases, suspension or expulsion.

Student Acceptance – please see form at end of this policy document

Information Technology (IT) Acceptable Use Policy

CBS Secondary School, Dungarvan has developed a comprehensive IT Acceptable Usage Policy.

The policy can be found on the homepage of the school's website, www.dungarvancbs.com.

We ask that you look up this document online and carefully read through it before signing to confirm that you have understood this policy. It is laid out in a very clear and concise manner to make to very easy for the reader to understand.

The aims of the policy are to:

1. Promote the professional, ethical, lawful and productive use of Dungarvan CBS's IT systems by explaining the dos and don'ts in the following areas:-
    - General use.
    - Emails.
    - Your Password.
    - Web access and content filtering.
    - Social media & Cyberbullying.
    - Responsible use of resources.
    - Monitoring.
    - Printing.
    - Data Protection GDPR.
2. To define unacceptable use and to state clearly how this policy will be enforced if it is breached.
3. To educate users about their IT Security responsibilities in relation to keeping passwords safe and any personal information of another person.

Student Acceptable Use Agreement

You are now asked to sign this policy in order to provide a record that you have read, understood and agreed to it.

If you do not understand or are unhappy with any part of this policy, please raise this with the Principal before signing. By signing below you are agreeing to the following:-

- I confirm that I have read and understand this IT Acceptable Use Policy
- I agree to abide by the conditions set out in this policy.
- I agree to the use of my photos or videos for assessment purposes.
- I accept that if the school considers it appropriate, my schoolwork, photo or video may be chosen for inclusion on the school website, school related print media, including newspapers.

Student's Signature:	
Print Name	
Date	

As the parent or legal guardian of the above student:

- I confirm that I have read the IT Acceptable Use Policy and grant permission for my son or the child in my care to access and use Dungarvan CBS's IT systems.
- I understand that the internet access is intended for educational purposes.
- I also understand that every reasonable precaution has been taken by the school to provide for online safety but the school cannot be responsible if students access unsuitable websites.
- I agree to the use of my son's photos or videos for assessment purposes.
- I accept that, if the school considers it appropriate, my son's schoolwork, photo or video may be chosen for inclusion on the school website, school related print media, including newspapers.

By signing below you are agreeing to the above:-

Parent/Guardian Signature:	
Print Name	
Date	

Please review the school's **IT ACCEPTABLE USE POLICY** and return your signed acceptance of this policy to the school with your Application Form.

Proposed by: _____ Chairperson: _____

Seconded by: _____ Date: _____