ST. VINCENT'S
CASTLEKNOCK COLLEGE

Digital Learning & Acceptable Usage Policy

1. Introductory Statement

This document sets out the policy of the school in respect of our Digital Learning and Acceptable Usage approaches. It has amalgamated, incorporated and subsequently supercedes the policies which were, heretofore, individualised in the 'Distance Learning Policy', 'Internet Acceptable Usage Policy' and the 'Privacy Policy'.

2. Scope of this Policy

This policy applies to all Digital Learners associated with Castleknock College i.e. users of computer and internet facilities in St Vincent's Castleknock College – students, teachers, administrative staff, other members of school staff and visitors using the school facilities.

The Internet is considered an information source for students and staff. It is used as part of curriculum instruction, administration and research. The Local Area Network allows students and staff to communicate and share information within the school. These technology resources and facilities, both hardware and software, are the property of St Vincent's Castleknock College and should be used solely for legitimate and authorised instructional, administrative and public service purposes.

In all cases students must use their @castleknockcollege.ie account to log in. Students are not to use any other account under any circumstances for the purposes of Digital Learning within the College.

The list of applications that will be used for Digital Learning will primarily be:

- Office365, incorporating:
    - Microsoft Outlook (e-mail)
    - Microsoft Teams
    - Microsoft OneNote

    - Microsoft Forms
    - Microsoft Stream
- Zoom – for live online classes.

There may be some additional applications that teachers may use, and the teacher will provide the student with the information required to access them. This must, in all cases, use an @castleknockcollege.ie account as the login.

3. Digital Learning Approach

Digital Learning will take what is known as a blended approach and some teachers may use different methods more than another teacher. For example:

- Some teachers may use regular live classes while others may not
- Some teachers may use live classes through Zoom while others may use Teams
- Some teachers may distribute work as weekly bulk assignments while others may do so as daily homework-style tasks.

In all cases the primary aim is to cover the required curriculum areas for their specific subject. The teacher will decide the most effective method to use to achieve this aim. Students should get in touch with their teacher right away if they are having difficulty with any aspect of their subject or if they are finding the workload unmanageable.

4. Digital Learning Responsibilities

(a) <u>For staff and teachers:</u>

- Teachers have overall control of the online interaction of their class.
- Disruptive students will be removed in order to allow those who wish to partake a fair chance to do so. Teachers will record any interruptions to the relevant Deputy using the Online Report Form. Repeatedly disruptive students may receive a temporary ban from all online access.
- Teachers will do their utmost to be available at the identified time on their timetable – this may be via a Zoom live video, through Teams chat or by e-mail.

(b) <u>For students:</u>

- Students are to communicate through your @castleknockcollege.ie account only. The use of any other account or e-mail address is expressly prohibited.
- Students must not engage in communications with any account other than an @castleknockcollege.ie account and report any such activity to your teacher or year-head's @castleknockcollege.ie e-mail account.
- Students must always be civil and respectful to your teachers and fellow students
- Students are not to record or forward any content within a Teams group – such as worksheets, exam papers, answers, solutions, videos, notes or Zoom links – to anyone else without the permission of the creator of that content
- Students understand that all your online activity is recorded. This includes anything you send or say via e-mail, Teams, Zoom and OneNote, and whether you are checking regularly for assigned work.
- Students understand that acceptable contact hours for communicating with a teacher(s) are generally timetabled hours. Students contacting a teacher(s) outside of these hours can expect a delayed response.

(c) <u>For parents:</u>

- Parents should ensure that their son is checking in regularly for assigned work.

- Where live classes are being run, parents should ensure their son is in an area of the house that is quiet and free from distractions. Please be mindful of Child Protection Guidelines, for example, bedrooms should not be used for live classes.
- Live online classes should be viewed by your son only.

Back to top

5. Live Online Classes

Teachers may deliver some of the course "live" using Zoom or Teams. This will use varying combinations of audio, video, virtual whiteboards and screencasts.

In the use of Zoom:

- Students must always follow the direction of their teacher just as in the classroom.
- Students are not to turn on their video at any time.
- Students are not to turn on their microphone unless the teacher invites them to do so. In any case, all microphones should be on mute when a person is not speaking to avoid distracting background noise being broadcast to everyone.
- A Zoom link is intended for the student only. The teacher will decide who should receive the link. Do not forward any link to anyone else.
- All Zoom sessions are recorded, and these recordings may be made available by the teacher to the class to watch back again later. This recording includes any video, screenshares, whiteboards and audio from the class.
- Only the teacher is allowed record a session. No-one else is permitted to record.

6. Data Privacy Statement

Our Digital Learning Policy incorporates the Internet Acceptable Usage Policy (AUP) 2018 and College Privacy Policy.

(a) <u>What we retain:</u>

- Login activity, specifically, the last time a student logged in to their Office365 account
- Within Teams and OneNote, the date and time of if/when a student views any assignments or OneNote notebooks set for them and when they submit any work for same
- In live classes using Zoom or Teams, all audio, video, whiteboard, annotations and screenshare activity of both teacher and participants (audio/video is not recorded if the student is on mute and the video is not enabled).

(b) <u>Why we retain it:</u>

- To assist us in making sure students are engaging in learning sufficiently and in good time
- To assist us in generating appropriate and relevant feedback to parents on progress
- To provide revision materials by means of replying topics covered in a live class, and to ensure those who might be unable to attend live classes can still cover the same content as the rest of the class
- To provide a record of activity in the event of a disciplinary or other issue arising during a live class.

(c) <u>Where we retain it:</u>

- All recordings are kept within the College's own systems which requires a valid @castleknockcollege.ie login to access
- The College's own systems are configured so that all data resides within an EU country only, which in the case of Office365, is Ireland.

(d) How long we retain it for:

- Ordinarily this is cleared at the end of each exam session, i.e. at the end of 3rd Year and at the end of 6th Year. In any case, activity and content will not be retained beyond the students exit from the College, either through early exit or through graduation.

Back to top

7. Implementation Strategies Within the College

The school employs several strategies in order to maximise learning opportunities and reduce risks associated with the Internet.

- Students will always treat others with respect and will not undertake any actions that may bring the school into disrepute.
- Internet sessions will always be supervised by a teacher.
- Students and teachers will be provided with training in the area of internet safety.
- A laminated poster of the Rules for Students will be displayed in all computer rooms and close to computer workstations in the classrooms.
- Virus protection software will be used and updated on a regular basis.
- Filtering software and/or equivalent systems will be used in order to minimise the risk of exposure to inappropriate material in conjunction with PDST Broadband.
- Personal Websites, Blogs, Gaming and Social Networking sites such as Facebook are blocked as are all inappropriate websites.
- Uploading and downloading of non-approved software is not possible due to security systems and must not be attempted.
- The use of personal devices, or other digital storage media in school requires a teacher's permission.
- Using college printers for printing of inappropriate or offensive material is not permitted and will be considered a violation of this policy.

Back to top

8. Internet Acceptable Use

(a) Board of Management

- To ensure that the policy is developed and evaluated over time.
- To approve the policy at a meeting of the Board.
- To consider reports from the Principal and relevant Post Holders on the implementation of the policy.

(b) Headmaster, Deputy Principal(s) and relevant Post Holders

- To oversee implementation of the policy.
- To establish structures and procedures for Acceptable Internet Usage

- To provide all staff - including teachers, resource teachers, supply staff, special needs assistants and administrative staff – as well as parents – with information on Acceptable Use and to explain its importance.
- To provide training for staff in the appropriate, ethical and responsible use of information technology.
- To ensure that users understand that failure to adhere to this Acceptable Usage will result in the loss of privilege and/or disciplinary action.
- To monitor the implementation of the policy.

(c) Teachers and Other Staff

- To accept the terms of the Acceptable Use before using any internet resource in the school.
- To instruct students in the appropriate use of computer and internet resources.
- To monitor the use of computer and internet resources.
- To record any violations of the Acceptable Use and inform the relevant authority.
- To impose appropriate sanctions for violations of the Acceptable Use, as outlined in the Parents Notification and Permission and in the school Code of Behaviour.

(d) Students

- To sign to an Acceptable Use agreement which is legally binding.
- To agree to exhibit responsible behaviour in the use of all resources.
- Take personal responsibility for not accessing inappropriate material on the internet.
- To accept that St Vincent's Castleknock College is not responsible for materials, or information of any kind, found or acquired on the network.
- To accept that violation of this Acceptable Use may result in access privileges being revoked and that appropriate school discipline and/or legal action may be taken at the discretion of St Vincent's Castleknock College.
- To accept that violation of the regulations in this policy may constitute grounds for legal action against the user, including, but not limited to, a criminal prosecution.

(e) Parents

- To become familiar with the school's Digital Learning Policy and to discuss it with their son.
- To sign the Parent Notification and Permission which allow students to use the computer and internet resources and to receive instruction in the appropriate use of these resources.
- To accept responsibility for supervision, if and when a student's use of e-mail and the internet is not in a school setting.

Parents are encouraged to support the school's Digital Learning Policy. Parents have the right to withdraw their sons from use of the internet in the school. This should be done by contacting the Headmaster and the teacher(s) involved in facilitating its use. The school takes every reasonable precaution, through the strict operation of this policy, to provide for online safety, but the school cannot be held responsible if pupils access unsuitable websites.

Back to top

9. Focused Areas of Concern

(a) The Internet

- Students will use the internet for educational purposes only.
- Downloading materials or images not relevant to their studies is in direct breach of the school's acceptable use policy.
- Students will not intentionally visit internet sites that contain obscene, illegal, hateful or otherwise objectionable materials.
- Students will report accidental accessing of inappropriate materials to the teacher in charge.
- Students will be taught to understand the concept of plagiarism, to acknowledge the sources of information and to respect copyright when using Internet material in their own work. Students will not copy information into assignments and fail to acknowledge the source, as to do so would be a copyright infringement.
- Students will be aware that any usage, including distributing or receiving information, school-related or personal, may be monitored in order to safeguard the security of the systems in the school and the good name of the College.

(b) Email

- Students are provided with a college email account under supervision by or permission from a teacher.
- Access in school to pupils' external personal email accounts will not be permitted.
- When sending emails, messages should be polite and sensible. Emails sent to external organisations should be written carefully and authorised before sending.
- Students will not send any material that is illegal, obscene, defamatory or that is intended to annoy or intimidate another person.
- Students will not disclose personal information – such as home addresses telephone numbers or pictures – about themselves, other students, relations or teachers in emails.
- Students will note that sending and receiving email attachments is subject to permission from their teacher.
- Pupils may download email attachments only with the teacher's permission and will first run a virus check
- Students will never arrange a face-to-face meeting with someone they know only through emails or the internet.
- The college reserves the right to block access to a student email account if in appropriate actions are being investigated.

(c) Internet Chat

- Skype, discussion forums and other electronic communication forums will be used for educational purposes only and will always be supervised.
- Students will have access to skype, discussion forums, messaging or other electronic communication only if they have been approved by the school.
- Private, pre-arranged, direct conferencing between the school and another school or suitable educational organisation will be permitted only under strict supervision.
- Face-to-face meetings with someone organised via internet chat is forbidden.
- Pupils will not be allowed access to public or unregulated chatrooms.

(d) School Communication Channels

- The website of St Vincent's Castleknock College will reflect the school's ethos.

- The Colleges' channels of communication will be regularly checked to ensure that there is no content that compromises the safety of pupils or staff. It will also be checked to see that no content denigrates an individual or might threaten the good name of the College and that the language and tone used is appropriate.
- Website using facilities such as guestbooks, noticeboards or weblogs will be checked frequently to ensure that they do not contain personal details.
- The school will endeavour to use digital photographs, audio or video clips focusing on group activities. Content focusing on individual students will not be published on the school website without parental permission. Video clips may be password protected.
- The school communication channels will avoid publishing the first name and last name of individuals in a photograph.
- Personal pupil information including home address and contact details will be omitted from school web pages.
- The school will ensure that the image files are appropriately named – and will not use pupils' names in image file names or ALT tags if published on the web.
- Pupils will continue to own the copyright on any work published.

(e) Personal Devices

- Students are responsible for their own technology within the school and on all school linked occasions. For example, leaving a mobile phone turned on or using it in class, sending nuisance text messages or the unauthorised taking of still or moving images with a mobile phone camera, are all direct breaches of the school's Digital Learning Policy.

(f) Cyber-Bullying

- Cyber-bullying is defined as using social network sites, internet, email, etc to demean, humiliate, exclude, or otherwise undervalue another person through direct or indirect methods.
- Any incident involving a student, current or recent past, as perpetrator or victim, is of concern, but especially when both perpetrator and victim are students, current or recent past. Equally, social comment about a member of staff which falls under the categories listed above will not be tolerated.
- St Vincent's Castleknock draws a distinction between incidents which originate from within the school environs and those which occur outside. While the same standards apply at all times and in all places, it needs to be recognised that the College cannot be held responsible for students' actions when not on the premises.
- The College takes seriously the responsibility of regularly informing students about internet protocol and best practice in the area of internet usage, including the concept of "public domain". The College values parents' support in reinforcing best practice in this area."

10. Structures Supporting the Acceptable Use Policy

- This Acceptable Use Policy will help students benefit in a safe and effective manner from the IT facilities offered by the schools. Internet use and access is considered a school resource and privilege. If the school AUP is not adhered to, this privilege will be withdrawn and appropriate sanctions will be imposed.

- 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 reserves the right to examine or delete any files, e-mail messages and their attachments that may be held on its computer system and to monitor any Internet sites visited. The Principal and/or Board of Management may view computer logs where misuse is detected.
- The school also reserves the right to report any illegal activities to the appropriate authorities.

11. Privacy Policy

St Vincent's Castleknock College (SVCC) is committed to protecting the individual's privacy and complies with the General Data Protection Regulation (GDPR) effective 25 May 2018 and other regulations. The following policy explains how and why we collect personal data and how it is used.

In summary, SVCC does not: collect more personal data than is necessary; use personal data for purposes other than those specified; keep personal data for longer than it is needed; or share personal data with unspecified third parties.

(a) Collection and use of data

While visitors can use the SVCC website without divulging personal information, when a person contacts us via an email or online form, SVCC collects and stores that information. The information provided (name, organisation, email address, phone number etc) will be processed and stored so that SVCC can contact and respond to the sender.

By supplying personal data to SVCC, an individual is consenting to the processing of such data as outlined in this privacy policy.

We collect personal data when a person requests the provision of SVCC services including meals, supervised study, private music tuition, school trips and any other services/products that may from time to be available on our website.

(b) We use this information to:

Provide and administer the service requested by parents/guardians/students and others.

Keep parents/guardians/students and others up to date with relevant SVCC information, services and events. For example, SVCC issues a weekly e-zine/newsletter known as the Headmaster's Bulletin directly to the email address of parents/guardians, the Board of Management, staff and others who wish to receive it.

(c) Monitor online traffic patterns and site usage (see Cookies below)

We do not share personal data with third parties for commercial or marketing purposes. Where data is shared with third parties, it is done so securely for administration purposes only.

Individuals have the right to opt-out of receiving SVCC communications at any time. To do so, e-mail info@castleknockcollege.ie or follow the 'unsubscribe' link contained in all SVCC electronic communications.

SVCC may use parents/guardians/students and others personal information to contact them with the school's e-zine (newsletter) and notices of events. SVCC may also use individual contact information in order to engage in research activities.

Materials and other information that parents/guardians/staff provide are shared with the following third parties: MailChimp (email automation platform) and delivery and postage providers.

SVCC reserves the right to share parents'/guardians'/staffs' and others' personal data if legally required to do so by a governmental or regulatory authority.

(d) Events and Photography/Images

At SVCC organised events including musicals, debates, sporting activities and other activities proper to a school, there may be photography or another image recording taking place. People who express a preference not to appear in images captured will be accommodated.

SVCC does not provide private contact details of any staff member, student, parent/guardian or others without the express permission of the individual in respect of whom the contact details have been requested.

(e) Data Security

SVCC uses appropriate technical and physical security measures to ensure the security of any personal data stored on our systems (online and paper files) and to protect from unauthorised access, loss, manipulation, falsification, destruction or unauthorised disclosure.

SVCC employs CCTV both for security of the staff and students and for the school premises and its installations. CCTV cameras are deployed and sited in compliance with GDPR privacy requirements and footage and images captured on CCTV are not shared with any third party unless required to do so by a governmental or regulatory body authorised to request such images

(f) Data Retention

Personal data collected and stored by SVCC is retained for no longer than necessary for the purpose for which it was collected. We recognise that personal data may not be retained indefinitely.

(g) Cookies

Some pages on the SVCC website use cookies, both for record-keeping purposes and to enhance the user experience by providing useful features. Cookies are small text files that act as an identification card, and they cannot be executed as code or deliver viruses. The use of cookies is an industry standard, their purpose merely being to record that you have visited or returned to that web page. We do not collect additional information such as age, gender, interests or bank details.

(h) Editing/Deleting personal data

If a person, whose personal data SVCC stores and processes, believes the data held is incorrect or out of date, please email info@castleknockcollege.ie so that the data can be updated.

If a person, whose personal data SVCC stores and processes, wishes their personal data to be deleted please email info@castleknockcollege.ie so that the data can be deleted within a month of receipt of request.

Please note that deleting stored data may have implications regarding future communications.

(i) Access to copies of personal data

Individuals have the right to request access to the personal data SVCC may hold. To make such a request, contact info@castleknockcollege.ie. SVCC will provide individuals with a copy of their personal data. To comply with such a request, we may request verification of identity of the person making the request. The request will be fulfilled by sending the data copy electronically unless the request expressly specifies a different method. The first request made by a customer is free of charge but may be subject to an administrative fee for further requests.

(j) Unsolicited information

SVCC not send out unsolicited information, including e-mail, regarding any third party commercial offers or advertisements.

(k) Linked sites

This Privacy Policy is applicable to the SVCC website only. Linked websites are not under the control of SVCC and the school is not responsible or liable for the contents of any linked site or any link contained in a linked site. Links are provided to you as a convenience, and the inclusion of any link does not imply the endorsement of the site by SVCC.

Neither are we responsible for the privacy practices of those websites. Always check the privacy policies of any sites visited. Once redirected to another website, this SVCC Privacy Policy is no longer applicable.

Changes to this policy

We may make changes to this privacy policy from time to time. All changes will be updated here, on this page. The date of the latest review can be found at the end of this Policy.

CONTACT:

If you require any further information on this Policy including data correction, amendment, erasure, restriction or portability, please contact info@castleknockcollege.ie using the reference Privacy Policy.

1) Ratification & Communication

This Digital Learning and Acceptable Usage Policy of St Vincent's Castleknock College has been ratified by the Board of Management. A short summary of the policy will be included in the yearly students' journal. Students and parents/guardians must sign the AUP permission form.

2) Implementation Date

This policy was ratified by the Board of Management at their meeting in March 2021.

3) Monitoring the Implementation of the Policy

Parents/guardians and all members of staff will be involved in monitoring the implementation of this policy.

4) Reviewing and Evaluating the Policy

There will be an annual evaluation through random surveys, drawn up by any of the three education partners, to ascertain adherence to the Digital Learning and Acceptable Usage Policy in the school. A full review of this Policy will be undertaken every three years.

Signed: Donal Hanlon

Chairperson of Board of Management

Date: 24 March 2021

Signed: Christopher Kinsella

Principal/Secretary to the Board of Management

Date: 24 March 2021