Hillfield Strathallan College
Learn with Joy. Live with Purpose.

Please note: HSC requires annual parental sign-off approval for the AUA. Students will also approve the AUA through a separate process.

Updated December, 2015

PROVIDING RESOURCES/SERVICES

1. IT resources/services include but are not restricted to school computers, the HSC network, First Class, the school telephone system, digital cameras and other multimedia resources. These resources/services support the resource-rich environment HSC provides to fulfil the educational policy of the College and to enhance the educational and professional experience of the users. IT resources/services including Internet and e-mail access are available to all students and Staff at the College. Students in Early Education programs (JK-Grd.2/M5-7) have access through Staff monitored accounts, but not through a personal ID system; students in Grades 3 to 12 have access through a personal ID and password system.

2. IT resources/services provided by HSC are not intended to replace equipment used in the home environment. HSC determines the quality and quantity of resources it will provide on campus and facilitates BYOD access. HSC's aim is to leverage the home and school connectivity as much as possible, within limitations determined by the College.

3. HSC provides IT resources/services for the following purposes

- for educational research and applications required by the academic and co-curricular programs
- to fulfil administrative duties as required by the program and College
- to enhance communications locally and globally

4. HSC provides resources/services for educational and professional use; HSC does not provide IT resources/services for personal use or personal recreation, including on-line games and shopping sites.

5. HSC reserves the right to limit access through personal IT equipment which may be connected to HSC resources (e.g. headphones, ipods, video games, laptops, X-BOX games, cell/video phones, DVD players, etc.)

- Exceptions may be considered with prior permission or approval by IT personnel or appropriate faculty
- HSC assumes no responsibility for personal IT equipment or personal downloaded resources that students or employees bring on campus; the individual is responsible for appropriate licensing, copyright considerations and downloaded material of any kind. HSC expects users to abide by legal requirements and does not support infringements.

INTERNET ACCESS AND USE OF IT RESOURCES

1. Acceptable Use

Internet access is provided to facilitate each person's role and responsibilities of an educational nature and may not be used to access inappropriate sites or used for non-educational communication or distribution that contains information or images of a pornographic, defamatory, demeaning, subversive, threatening or racially offensive nature, or that otherwise offend College policies, privacy or copyright laws, the Ontario Human Rights Code or the Criminal Code of Canada, even under the guise of research.

These expectations are consistent with general College guidelines in the student handbook, the Code of Conduct and the professional policy documents for employees.

2. Unacceptable Use

Withdrawal of services and disciplinary action may apply for infractions to IT use affecting the educational mission and policy, the code of ethics and behaviour regarding manners, discipline, harassment, theft, privacy regulations, academic honesty, respect for property and the environment and professional policy. Consequences for infractions will be consistent with processes and standards of practice according to the College handbook for students and the professional practice documents for employees. The extent of withdrawal of privileges for IT resources/services will vary depending on the severity of the infraction. For users whose IT privileges are withdrawn, their signed Acceptable Use Agreement, valid at the time of the infraction, becomes null and void; users will have to sign a new agreement if and when reinstatement applies.

It is important to note that withdrawal of services for student user accounts could have serious implications on their ability to complete course requirements and may have a negative impact on academic achievement.

GUIDELINES FOR ACCEPTABLE AND UNACCEPTABLE USE OF IT RESOURCES

1. A Responsible User <u>Will</u>:

• use the IT resources/services for educational or professional purposes in support of and consistent with the mission and educational policy of HSC
• use the IT resources/services for local and external electronic communication
• use only software officially licensed by the College or personally for BYOD access
• respect school property for the benefit of all users
• respect that resources/services are shared by many users and will therefore use resources/services effectively and efficiently and conserve resources/services, especially for printing and electronic file storage and management
• keep her/his personal password private and use only his/her own account
• take precautions to ensure that other users may not gain unauthorized access to his/her account
• understand and appreciate that his/her use of IT resources/services can have an impact on other users

2. A Responsible User <u>Will Not</u>:

• violate accepted policies, practices or codes of conduct of the College
• compromise his/her own or another person's security by posting personal pictures or information on a web page through any device
• use IT resources/services for any illegal purpose (federal, provincial or applicable court order)
• install personal software on HSC computers
• connect personal electronic devices, laptops or software to HSC equipment without permission or beyond the accepted terms of accessibility
• use impolite, inappropriately suggestive or abusive language or contravene the harassment policy
• engage in cyberbullying at any time as a viewer or a sender of electronic images, texts, information, documentation, links or other forms of communication
• change or use computer files that do not belong to the user
• use, send, or receive copyrighted material without the required permission
• share his/her personal password with anyone
• leave network connections open
• enter or attempt to enter restricted network locations
• use excessive data space or bandwidth that may limit the access of other users

EDUCATIONAL SUPPORT, LICENSED ACCOUNTS, SOCIAL NETWORKING

1. HSC Faculty have a professional responsibility to work together to help students develop the skills needed to discriminate among information sources, to identify information appropriate to their age and stage, and to evaluate and use information to meet their educational goals.

2. Licensed Accounts for educational third party software – age restrictions for students under 18 years. In support of student internet safety and to meet standard terms of use for educational web based software accounts, parents/guardians are required to authorize teachers in providing accounts for software the College deems appropriate for research purposes for students under age 18 years. This applies to software recommended by the Learning Commons staff for research purposes and for resources sourced by classroom teachers. Faculty and staff are responsible for applying the terms of use for any resources used by students at the College. Teachers are not responsible for accounts that are set up by students personally or by their parents which are beyond those resources recommended by the school and are used in or outside of the school.
By signing the AUA on behalf of your child, you are agreeing to provide this authorization for teachers to set up accounts for students and to provide access to online resources for educational purposes. Please note that parents/guardians are responsible for supervising their child's access to the HSC account when it is used outside of school.

3. Use of Personal Social Networking Sites
The College respects that staff and students use social media and networking sites, as well as personal websites and blogs for their own personal purposes. However, the personal use of these sites by staff and students must not involve communications or activities that represent a breach of the values, policies and codes of conduct that apply to staff and students. These policies include, but are not limited to the Code of Conduct, Professional Practices Standards, Respect at the College, and others that promote respect for the well-being, security and privacy of members of the College community.

Users should exercise care in setting appropriate boundaries between their personal and public online behaviour, understanding that what is private in the digital world often has the possibility of becoming public, even without their knowledge or consent. The College strongly encourages all users to carefully review the privacy settings and terms of use on any social media and networking sites they use (such as Facebook, Twitter, LinkedIn, Instagram, etc.), and exercise care and good judgment when posting content and information on such sites. When using a social media site, employees may not include current students as "friends", "followers" or any other similar terminology used by various sites. If an employee has a community that extends to persons who are parents, alums, or other members of the community, s/he must exercise good judgment about any content that is shared on the site.

Additionally, users should adhere to the following guidelines, which are consistent with HSC standards on harassment, student relationships, conduct, professional communication, and confidentiality:

• a user should not make statements that would violate any HSC policies, including its policies concerning discrimination or harassment
• a user must uphold the College's value of respect for the individual and avoid making defamatory statements or posting inappropriate images about the College, its employees, its students, or their families
• any user may not disclose any confidential information of the College or confidential information obtained during the course of his/her employment/enrolment, about any individuals or organizations, including students and/or their families. If HSC believes that a user's activity on a social networking site, blog, or personal website may violate the College's policies, the College will take action and may request that the user cease such activity. Depending on the severity of the incident, the user may be subject to disciplinary action up to and including withdrawal of services, expulsion or termination.

NETWORKED ACCOUNTS
1. Access
• networked accounts are a PRIVILEGE, not a right
• users must use IT facilities and resources/services only for the purpose for which they were authorized
• wireless access is provided to support educational requirements within the BYOD model and HSC prescribed resources

2. User Responsibility
The person to whom an account is issued is responsible at all times for its proper use.

Users:
• must protect their passwords; sharing passwords or accounts is not acceptable
• may keep an HSC network account as long as the user is an employee or student in good standing at HSC
• for personal security, must never reveal their personal address or phone number or that of other students or colleagues in the networked system
• must not use the College's resources for ongoing personal business or gain

3. Monitoring Network Accounts – safety and ethical use
• The College is the sole owner of all information stored on the school's information systems. This includes files, programs, electronic mail stored on school computers, as well as any data or message transmitted via the HSC network, including the HSC cloud. Confidentiality must be adhered to within the user's role and responsibility at the College.
• IT Services will have access to all user accounts, including e-mail and will monitor user accounts on a random basis to ensure reliability, stability and accepted use of resources.
• IT Services Staff may close an account at any time as a result of an infraction to the agreed use, as approved by the Director of Operations and/or the School Principal.

MAINTAINING SYSTEMS & RESOURCES
1. Reliability
While HSC is responsible for ensuring a high level of system reliability and maintains a strong backup system, HSC is not responsible for any damages or loss sustained by the user. This includes loss of data resulting from delays, non-deliveries, misdeliveries or service interruptions. Users are responsible for backing up their own files and using assigned drives and managing file storage via USB drives or other appropriate systems effectively and efficiently. HSC assumes no responsibility for the accuracy or quality of the information obtained through the Internet.

2. Security
Security on any computer system is a high priority. If a user feels he/she can identify a security problem on the HSC network, he/she is required to notify the School Principal or the Director of Operations. The user must keep the problem confidential and keep the personal password private. Any user identified as a security risk will be denied access to the HSC network; the signed AUA of the user will become null and void when the risk is formally identified. Consequences will apply as appropriate for an identified infraction based on published policies, formal consultation and/or precedent.

3. Vandalism
Acts of vandalism may result in cancellation of privileges. Vandalism is defined as any attempt to harm or destroy the College's hardware, software, peripherals, infrastructure, or an individual's resources which are part of the BYOD program, the data of another user, the HSC network or any of the networks connected to the Internet. This includes, but is not limited to, the uploading/downloading or the creation of computer viruses.

POLICIES AND GUIDELINES ARE SUBJECT TO CHANGE ACCORDING TO THE NEEDS OF INFORMATION SERVICES AT THE COLLEGE. USERS WILL BE NOTIFIED APPROPRIATELY. INQUIRIES MAY BE DIRECTED TO CHIRS KWIECIEN, DIRECTOR OF OPERATIONS.