



AP-H-201.1 Use of Information and Communication Technology Administrative Procedures

REVISED October 24, 2016

BACKGROUND

FFCA recognizes:

- the use of information and communication technology, including social media, can provide increased access to teaching, learning, communication and collaboration opportunities for both students and staff.
- the opportunities that technology can provide also come with a responsibility to use technology in a manner that promotes the potential benefits while maintaining a safe and caring learning environment.
- that developing digital citizenship competencies is essential to student preparation.
- that social media can provide highly effective means of communicating to parents about teaching and learning at FFCA.

DEFINITIONS

1. Technology Resources include technology infrastructure, devices, software and services (including network and internet access) owned and operated by FFCA.
2. Internet-based services (also known as cloud services) refer to any online service or digital information storage and applications provided by organizations or vendors other than FFCA.
3. Portable storage device refers to any mobile device that can store, process or transmit information digitally including, but not limited to laptops, tablets, smartphones, flash drives, CD/DVD.
4. Personal Information under the Freedom of Information and Protection of Privacy (FOIP) Act, “personal information” means recorded information about an identifiable individual including:
 - a. the individual’s full name, home or business address or home or business telephone number,
 - b. the individual’s race, colour, national or ethnic origin, religion, political beliefs or associations,
 - c. the individual’s age, sex, marital status or family status,
 - d. an identifying number, symbol or other particular assigned to the individual,
 - e. the individual’s fingerprints, or other biometric information, blood type, genetic information or inheritable characteristics,
 - f. information about the individual’s health and health care history, including information about a physical or mental disability, or socio-emotional well-being,
 - g. information about an individual’s academic performance including assessment information, anecdotal reports, behavioural incidence reports and attendance,
 - h. information about the individual’s educational, financial, employment or criminal history, including criminal records where a pardon has been granted,
 - i. the individual’s personal views or opinions or anyone else’s opinion about the individual.

PROCEDURES

FFCA supports and encourages the purposeful integration of technology to enhance and facilitate student achievement and character development and strives to develop and maintain the technology infrastructure, tools and staff capacity to enable such integration.

1. Educational Technology Integration

- 1.1. Principal Educators are responsible for overseeing the infusion of technology and learning in conjunction with the Chief Operations Officer (COO) and the Director of Technology Services (DTS). This shall be conducted in a manner consistent with FFCA philosophy, educational goals, guidelines, and the FFCA *Technology User's Reference Guide*.
- 1.2. An Educational Technology Committee (ETC) consisting of the COO, DTS and one teacher from every site will be created with the purpose of:
 - 1.2.1. Informing the growth of teaching and learning through the use of educational technology in ways that support FFCA's core values and guiding principles;
 - 1.2.2. Gathering, researching, and assessing information about existing and emerging educational technologies, and to explore their relevance to curriculum and pedagogical endeavors;
 - 1.2.3. Learning and modelling best pedagogical practices integrating educational technology;
 - 1.2.4. Providing guidance to staff in the integration of educational technology into practices and professional development;
 - 1.2.5. Providing continuous feedback on specific educational technology solutions.
 - 1.2.6. Being an addition liaison between the COO & DTS and campus administration and staff.

2. Technology Planning

- 2.1. Each campus will, in collaboration with the COO & DTS, develop a technology plan congruent with campus educational objectives, global FFCA educational goals and available Technology Services resources.
- 2.2. A technology refresh plan for renewal of campus technology resources will be developed and implemented by Technology Services in conjunction with campus administration. This plan will provide for regularly scheduled replacement of designated technology components as determined by campus administration and the DTS.
- 2.3. A Technology Advisory Group (TAG) consisting of the COO, DTS and one administrator from every site will be created with the purpose of:
 - 2.3.1. Ensuring that technology directions and educational goals are as congruent as possible,
 - 2.3.2. Facilitating the strategic, ordered, and cost-effective use of educational technology solutions and related resources,
 - 2.3.3. Guiding the evaluation, selection and ongoing usage of technology solutions throughout FFCA,
- 2.4. The DTS, in partnership with the COO and the Technology Advisory Group, shall develop a three year jurisdiction technology roadmap. This three year technology roadmap shall be available to FFCA Administration annually for feedback, review, modification and validation.

3. Management of Network Resources

- 3.1. All infrastructure work will be coordinated through Technology Services which will establish technical and process standards for the work.
- 3.2. Hardware purchases and installation must be done by, or in consultation with Technology Services and, where appropriate, the COO.
 - 3.2.1. Where appropriate a menu of approved devices in various categories will be developed from which devices for purchase will be selected.
- 3.3. Software purchases and installation on key administrative (office) and student-use devices and must be done by, or in consultation with, Technology Services, subject to the following conditions:
 - 3.3.1. Key Administrative (Office) Computers will be identified by Technology Services and their identities communicated to site administrators. They are those that are required for primary business operations of the school and site.
 - 3.3.2. Appropriate licensing will be obtained prior to activating an installation.
 - 3.3.3. Evidence of all software licenses purchased by a school or department will be readily available for audit.
 - 3.3.4. All software must be registered in the name of Foundations for the Future Charter Academy.
 - 3.3.5. No personal software may be installed without the consent of Technology Services.
- 3.4. A base image and software profile will be installed on all teacher/administrator devices as determined by the TAG in consultation with ETC and DTS:
 - 3.4.1. A description of the programs/applications approved as part of the base image will be made available to all staff.
 - 3.4.2. Updates to the base image and software profile will be done regularly by Technology Services.
 - 3.4.2.1. Updates to the base image and software profile will be done in a phased approach.
 - 3.4.2.2. When appropriate the schedule of phased installations will be communicated to administrators.
 - 3.4.3. Additional software that deviates from the established standards can be installed on an FFCA-owned device by designated campus resource at their own risk according to the following conditions:
 - 3.4.3.1. Staff members should only use programs developed and distributed by reputable providers
 - 3.4.3.2. Tech Services is to be consulted to determine any known software conflicts or security concerns prior to the installation of software, as well as obtain confirmation of whether or not existing licenses are already available that have already been purchased by FFCA.
 - 3.4.3.3. Appropriate licensing will be obtained prior to activating an installation.

3.4.3.4. Evidence of all software licenses purchased by a staff member will be readily available for audit.

**Should problems such as interoperability or security issues occur with a device that has 'non-standard' software installed, Technology Services will re-image the device to the base image and software profile. All other applications and data will be lost in this process.*

3.4.4. In specific cases, a user with an FFCA-owned laptop may be granted administrative access on their device, at the discretion of the DTS and COO.

3.5. All electronic messaging, digital storage, network access and any associated technology resources are provided by and the property of Foundations for the Future Charter Academy. As such any of these resources may be monitored, audited or reviewed at any time to ensure student safety, system integrity, adherence to FFCA Administrative Procedures or required legislative compliance.

4. Access to FFCA Network Resources

4.1. FFCA Technology resources should be used for purposes defined by the learning process or related support functions. Appropriate personal use is permitted as outlined in the *Information and Communication Technology (ICT) Acceptable Use Agreement*.

4.2. Use of FFCA-owned Resources

4.2.1. All FFCA-owned technology resources, including but not limited to hardware, software or proprietary data, are the property of Foundations for the Future Charter Academy. Use of these resources is subject to FFCA Administrative Procedures.

4.2.2. Any loss or damage to FFCA technology resources which occurs from actions contrary to the terms of FFCA Administrative Procedures is the sole responsibility of the user.

5. Use of Personal Electronic Devices at FFCA and on FFCA Network

5.1. Access to technology resources with personal devices shall subject to the following conditions:

5.1.1. There will be no violation of licensing agreements.

5.1.2. FFCA assumes no liability for damage or loss to personal devices.

5.1.3. Technical support for personal devices is not the responsibility of FFCA Technology Services.

5.1.4. It is the user's responsibility to ensure any personal devices accessing FFCA technology resources shall have a passcode assigned to protect the security of FFCA data.

5.1.5. Student use of personal electronic devices is to be in accordance with expectations of campus administration and staff

6. Network Use Agreements

6.1. All staff, students, directors, and other (community) users of FFCA network resources must sign the respective *Information and Communication Technology (ICT) Acceptable Use Agreement*.

6.1.1. Signed *Information and Communication Technology (ICT) Acceptable Use Agreement* for each staff member will be placed in permanent files at Central Office. The human resources department is responsible for maintaining permanent files. Staff and guest teachers will sign the form at the time of employment.

- 6.1.2. As part of the yearly registration or re-registration package, parents and students will be required to read and agree to the terms indicated within the student network use agreement. The Principal Educator is responsible for ensuring that the *Information and Communication Technology (ICT) Acceptable Use Agreement* is reviewed with students during the first week of school each year.
 - 6.1.3. Signed *Information and Communication Technology (ICT) Acceptable Use Agreement* for each director will be filed at Central Office with the human resources department. Directors will sign the form at the time of their election/appointment to the Board.
 - 6.1.4. Signed *Information and Communication Technology (ICT) Acceptable Use Agreement* for each community member (including parents) who use FFCA network resources will be filed at Central Office with the human resources department. Community members will sign the form at the time of their first use of network resources.
- 6.2. Review of the *FFCA Technology User's Reference Guide* will be the responsibility of the COO in consultation with the TAG, ETC and DTS and shall occur a minimum of once per year prior to re-registration. Each time the *FFCA Technology User's Reference Guide* is revised, the COO will inform administration of the changes to the document for dissemination amongst their staff, students and other relevant users.

7. Intellectual Property and Copyright

- 7.1. All users of network resources are required to respect copyright/licensing laws and regulations. The Board will not accept responsibility for a user who willfully and knowingly contravenes copyright or licensing laws.
- 7.2. Works covered by copyright that are developed by employees in the course of their employment shall be the intellectual property of the Board.

8. Information Security

- 8.1. All personal information collected by FFCA shall be stored and protected against unauthorized access.
- 8.2. Portable storage devices (including laptops) shall NOT be used to store any personal information about staff or students UNLESS it is:
 - 8.2.1. authorized by the Superintendent or designate
 - 8.2.2. encrypted and password protected on an FFCA-owned mobile device that has DTS-approved encryption enabled, or utilizes a service or device approved by DTS
 - 8.2.3. removed immediately following completion of task.
- 8.3. Use of cloud-based applications or cloud storage must not include data that contains personal information of staff or students UNLESS:
 - 8.3.1. The privacy agreement with the service provider provides for suitable levels of privacy and information security consistent with Alberta's FOIP legislation as determined by the DTS and Superintendent.
 - 8.3.2. The agreement is to provide for the security of as well as backup/disaster recovery of data stored to a standard that is determined to be acceptable by DTS (e.g. SAS70 or CICA 59790 compliance).
 - 8.3.3. Any data accessed or transferred is encrypted and password protected using enterprise-grade encryption that is determined to be acceptable by DTS.
 - 8.3.4. The privacy agreement is approved by the Superintendent or designate.

- 8.4. FFCA staff must report any breaches of information security, whether actual or suspected, to their immediate supervisor for investigation. Supervisors are to consult with the DTS for assistance. All privacy breaches are to be reported to the Superintendent or designate.

9. Social Media

- 9.1. Social media are specific types of cloud-based applications which include web-based and mobile technologies used for interactive dialogue including, but not limited to: personal websites, blogs, micro-blogs, wikis, podcasts, image and video sharing platforms.

9.2. User Responsibility

9.2.1. All users are personally responsible for the content/information they publish online

9.2.2. Social media used for educational purposes is an extension of the classroom and online behavior shall reflect the same standards of character expected in respectful face-to-face classroom interactions and adhere to the principles of digital citizenship. *What would be deemed unacceptable in a classroom is unacceptable online.

9.2.3. All social media postings should be considered to be in the public domain.

9.2.4. Staff members are responsible for moderating all published social media content related to classroom work.

9.2.5. Staff members shall insure that all postings:

9.2.5.1. express their individual points of view in a manner consistent with the professional expectations of their role

9.2.5.2. express their individual points of view in a manner which positively contributes to the mission of FFCA,

9.2.5.3. do not purport to represent the official views of FFCA (unless authorized to do so by Superintendent or designate).

9.2.5.4. do not express contrary views or concerns about FFCA or its stakeholders. (These should be expressed through appropriate internal avenues rather than through public forums.)

9.2.5.5. do not disclose information that would be considered confidential or proprietary information of FFCA without prior written approval of the Superintendent or designate,

9.3. Profiles and Identifying Information

9.3.1. No personal or identifying information about students, as defined in Alberta FOIP legislation and/or in this AP document, is to be posted on social media sites.

9.3.2. Photographs and video images must respect person's right to privacy and reflect content appropriate for educational purposes.

9.3.2.1. In sharing photographs or video images of students in which their face(s) are identifiable, parental consent is required through the Media Exposure section of our re-registration website. (Refer to 9.5.2 in this AP.)

9.3.2.2. In addition to verifying that digital consent has been obtained, staff must inform parents that their child's image will be used on social media for the duration of the school year.

9.4. Staff Use of Social Media For FFCA Purposes

9.4.1. Any use of social media accounts to be used by staff members for the sole purpose in their role with FFCA (i.e. class twitter accounts, blogs, etc...) shall be established expressly for that use and not be used for personal matters.

9.4.2. Use of official FFCA logo and wordmark is permissible within accounts established by staff members for the sole purpose in their role with FFCA as long as it is consistent with *AP-J-201.1 Brand Standards Guide*.

9.4.3. Prior to using social media accounts for school, campus or classroom purposes:

9.4.3.1. the social media guidelines in the *Technology User's Reference Guide* are to be reviewed and clarification sought from the Director of Educational Technology if necessary.

9.4.3.2. the Principal Educator or Supervisor must be informed

9.4.3.3. a *Social Media Account Information Form* must be submitted to the COO upon the creation of a new account, whenever access information is changed and at the commencement of a new school year.

9.4.4. All links to Social Media for FFCA classroom purposes are to be posted on the designated classroom platform as identified in the *Technology User Reference Guide*.

9.4.5. Upon request, login information and written consent to access these accounts must be provided to the Principal Educator or Supervisor. Staff are encouraged to use their FFCA email address as login ID for these accounts if possible.

9.5. Official FFCA & Campus Social Media Accounts

9.5.1. FFCA will maintain and manage the following official social media accounts:

9.5.1.1. FFCA Facebook

9.5.1.2. FFCA Twitter

9.5.1.3. Campus Twitter

9.5.2. FFCA will establish Active Directory accounts to be used to manage official FFCA social media accounts.

9.5.3. Campus administrators will be responsible for ongoing management and use of campus-based social media accounts.

9.5.4. The COO, in coordination with the CEO, Coordinator of Instruction and Coordinator of School Services will be responsible for the ongoing management and use of FFCA-based social media accounts.

9.6. Student School-based Use of Social Media

9.6.1. Teacher-directed use social media must be preceded by:

9.6.1.1. determination of the instructional value and conditions of use

9.6.1.2. instruction on the terms of use under which the application is being provided by the source,

9.6.1.3. instruction in digital citizenship,

9.6.1.4. communication with parent(s) and/or guardians regarding the instructional value of student use of social media.

9.6.2. Parental consent in the Media Exposure section of the re-registration website is required before students use social media. This includes:

9.6.2.1. in cases where photographs or video images of students in which they are identifiable are to be posted

9.6.2.2. in cases where student work is to be shared in an environment open beyond the FFCA community

*This consent may, but does not need to, be on an application-by-application (use-by-use) basis but specific consent may be required for social media use if application(s) have a sufficiently high profile and/or level of controversy. If uncertain, teacher should consult with campus or system administration. A parent may also agree to only provide consent for a specific use. In these instances a note should be made on the *Student Digital & Social Media Use Consent Form* or a specific-use consent form should be used.