CYBERSAFETY AT JCSS

CYBERSAFETY EMPLOYEE USE AGREEMENT FOR ALL JCSS EMPLOYEES

This document is comprised of this cover page and two sections (Section A and B):

Section A: Important Cybersafety Initiatives and Rules

Section B: Some Important Employee Obligations Regarding Student Cybersafety

Important terms used in this document:

(a) ***'Cybersafety'*** *refers to the safe use of the Internet and technology equipment/devices, including mobile phones*

(b) ***'School Technology'*** *refers to the school system's computer network, Internet access facilities, computers, and other school system technology equipment/devices as outlined in (d) below*

(c) *The term* ***'Technology equipment/devices'*** *used in this document, includes but is not limited to; computers (such as desktops, laptops, PDAs), storage devices (such as USB and flash memory devices, CDs, DVDs, floppy disks, iPods, MP3 players), cameras (such as video, digital, webcams), all types of mobile phones, gaming consoles, video and audio players/receivers (such as portable CD and DVD players), and any other, similar, technologies as they come into use*

(d) *'**Objectionable**' in this agreement means material that deals with matters such as sex, cruelty, or violence in such a manner that it is likely to be injurious to the good of students or incompatible with a school system environment. This is intended to be inclusive of the definition used in the Films, Videos and Publications Classification Act 1993.*

SECTION A
IMPORTANT JCSS CYBERSAFETY INITIATIVES AND RULES

The measures to ensure the cybersafety of JCSS outlined in this document are based on our core values.

The school system's computer network, Internet access facilities, computers and other school system technology equipment/devices bring great benefits to the teaching and learning programs at JCSS, and to the effective operation of the school system.

The overall goal of the school system in this matter is to create and maintain a cybersafety culture which is in keeping with the values of the school system, and legislative and professional obligations. This use agreement includes information about your obligations, responsibilities, and the nature of possible consequences associated with cybersafety breaches which undermine the safety of the school system environment.

Students are provided instruction in appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. School staff members receive Georgia Cybersafety Initiative (GaCSI) School Staff Training. This training is designed to provide the knowledge and skills necessary to create awareness and provide education about digital citizenship to K-12 students. Records are maintained to verify participation of student and staff trainings.

1. Cybersafety Use Rules

    1.1 All employees, students and volunteers, *whether or not* they make use of the school system's computer network, Internet access facilities, computers and other technology equipment/devices in the school system environment, will obey the cybersafety agreement.

    1.2 The school system's computer network, Internet access facilities, computers and other school system technology equipment/devices are for educational purposes appropriate to the school system environment. Employees may also use school system technology for professional development and personal use which is both reasonable and appropriate to the school system environment. This applies whether the technology equipment is owned or leased either partially or wholly by the school system, and used on *or* off the school site.

    1.3 Any employee who allows another person to use the school technology, is responsible for that use.

2. The use of any privately-owned/leased technology equipment/devices in the school system, or at any school system-related activity must be appropriate to the school system environment. This includes any images or material present/stored on privately-owned/leased technology equipment/devices brought onto the site, or to any school system-related activity. This also includes the use of mobile phones.

3. When using school system technology, or privately-owned technology on the school system site or at any school system-related activity, users must not:

    - Initiate access to inappropriate or illegal material
    - Save or distribute such material by copying, storing, printing or showing to other people.

4. Users must not use any electronic communication (e.g., email, text) in a way that could cause offense to others or harass, bully, or harm them, put anyone at potential risk, or in any other way be inappropriate to the school system environment.

5. Employees are reminded to be aware of professional and ethical obligations when communicating via technology with students outside school hours.

6. Users must not attempt to download, install or connect any software or hardware onto school system technology equipment, or utilize such software/hardware, unless authorized by the Technology Department.

7. All material submitted for publication on the school system website/intranet(s) should be appropriate to the school system environment. Such material can be posted only by those given the authority to do so by their administrator.

8. All school system technology equipment/devices should be cared for in a responsible manner. Any damage, loss or theft must be reported immediately to the Technology Department.

9. All users are expected to practice sensible use to limit waste of computer resources or bandwidth. This includes avoiding unnecessary printing, unnecessary Internet access, uploads or downloads.

10. The users of school system technology equipment and devices must comply with the Copyright laws and any licensing agreements relating to original work.

11. Passwords must be strong, kept confidential and not shared with anyone else.

12. Users should not allow any other person access to any equipment/device logged in under their own user account.

13. The principles of confidentiality and privacy extend to accessing, inadvertently viewing or disclosing information about employees, or students and their families, stored on the school network or any technology device.

14. Dealing with incidents

14.1 Any incidents involving the unintentional or deliberate accessing of inappropriate material by employees or students must be recorded in handwriting with the date, time and other relevant details.

In the event of access of such material, users should:

1. Not show others
2. Close or minimize the window, and
3. Report the incident as soon as possible to the Technology Department.

14.2 If an incident involves inappropriate material or activities of a serious nature, or is suspected of being illegal, it is necessary for the incident to be reported to their administrator IMMEDIATELY.

14.3 Any incidents involving the harassment, bullying, or harm to another individual must be recorded in handwriting with the date, time and other relevant details and be reported to their administrator IMMEDIATELY.

15. Any electronic data or files created or modified on behalf of JCSS on any technology, regardless of who owns the technology, are the property of JCSS.

16. Monitoring by the school system

16.1 The school system may monitor traffic and material sent and received using the school system's technology infrastructures.

16.2 The school system reserves the right to deploy filtering and/or monitoring software where appropriate to restrict technology access to certain sites and data, including email.

16.3 Users must not attempt to circumvent filtering or monitoring.

17. Breaches of the agreement

17.1 A breach of this use agreement may constitute a breach of discipline and may result in a finding of serious misconduct. A serious breach of discipline would include involvement with objectionable material, antisocial activities such as harassment or misuse of the school system technology in a manner that could be harmful to the safety of the school system or call into question the user's suitability to be in a school environment.

17.2 If there is a suspected breach of the use agreement involving privately-owned technology on a school system site or at a school system-related activity, the matter may be investigated by the school system. The school system may request permission to audit that equipment/device(s) as part of its investigation into the alleged incident.

18. The school system reserves the right to conduct an internal audit of its computer network, Internet access facilities, computers and other school system technology equipment/devices, or commission an independent audit. If deemed necessary, this audit will include any stored content, and all aspects of its use, including email. An audit may include any laptops provided by the school system or provided by the Department of Education.

Please note that conducting an audit does not give any representative of JCSS the right to enter the home of school system personnel, nor the right to seize or search any technology equipment/devices belonging to that person, except to the extent permitted by law.

19. Questions or concerns

19.1 Employees should take any questions or concerns regarding technical matters to the Technology Department.

19.2 Questions or concerns regarding other cybersafety issues should be taken to the Technology Department or your administrator.

19.3 In the event of a serious incident which occurs when the Technology Department or your administrator are not available, another member of your administration should be informed immediately.

SECTION B
SOME IMPORTANT EMPLOYEE REQUIREMENTS REGARDING STUDENT CYBERSAFETY

1. Employees have the professional responsibility to ensure the safety and welfare of children using the school system's computer network, Internet access facilities, computers and other school system technology equipment/devices on the school system site or at any school system-related activity.
2. If employees are aware of any students who have not received a copy of the cybersafety agreement, their names should be reported to the principal.
3. Employees should guide students in effective strategies for searching and using the Internet.
4. While students are accessing the Internet in a classroom situation, the supervising employee should be an active presence.
6. Employees should support students in following the Student Cybersafety Use Agreement. This includes:
    a. Verifying that all students in their care understand the requirements of the student agreement
    b. Regularly reminding students of the contents of the use agreement, and encouraging them to make positive use of technology.