St. John’s Lutheran School

TechSafe Plan

Technology Guidelines and Procedure for Staff and Students

Created: April , 2014
Last Revised:

Introduction

St. John's Lutheran's 21st century assets are seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, we discovered we need to build in the use of these technologies in order to arm our young people with the skills necessary to safely access lifelong learning.

Information and Communications Technology covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- Email
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading

While all are exciting and beneficial both in and out of the context of education, much of ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet and web-based technologies.

At ***St. John's Lutheran School,*** we understand the responsibility to educate our pupils on TechSafe issues; teaching them the appropriate conduct and critical thinking skills to enable them to remain both safe and responsible when using the internet and related technologies, in and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement (for all staff, administration, visitors and students) are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, webcams, SmartBoards, thin clients, iPads, digital cameras, etc.)

Disclaimer: Due to the constant changes taking place within technology, this policy may not contain the most recent developments. We will however, add any important issues to the policy when deemed necessary.

Roles and Responsibilities

As TechSafe is an important aspect of strategic leadership within the school, the administration, teachers and staff will have ultimate responsibility to ensure that the policy and practices are monitored and enforced. The named TechSafe co-coordinators at our school are Kay Koenitzer and 2 teachers to be named by August 2014. All members of the St. John's community will be made aware of who holds this position. It is the role of the TechSafe co-coordinators to collaborate and research current issues and up-to-date strategies to keep our St. John's community safe and moving forward.

The goal of this policy, supported by the school's acceptable use agreements for staff, administration, visitors and students, is to protect the interests and safety of the whole SJLS community.

Digital Citizenship

These procedures are written to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy: successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff online behavior are no different than face-to-face interactions.

TechSafe Resources for Teachers, Staff and Administration

- Our staff receives regular information and training on TechSafe issues
- Details and topics of the ongoing staff training is developed and implemented by the co-coordinators.
- **All** staff (including new staff members) receive information on the school's acceptable use policy
- All staff have been made aware of individual responsibilities relating to the safety of children within the context of technology and know what to do in the event of misuse of technology by any member of the school community
- All staff are encouraged to incorporate TechSafe activities and awareness within their curriculum areas and when using technology in their classroom.

TechSafe in the Curriculum

- The school provides opportunities within a range of curriculum areas to teach about our TechSafe policy and technology safety in general.
- Educating students on the risks and misuse of technologies that may be encountered in and outside of the school setting.
- Students are taught about copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- Students are aware of the impact of online bullying and know how to seek help if they are affected by these issues. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent, guardian, teacher or other trusted staff member.
- Students are taught to critically evaluate materials and learn good searching and online research skills across curricular teacher models, discussions and via the technology curriculum.

Password Security

All users must read and sign an Acceptable Use Agreement/Rules of Conduct Code to demonstrate that they have understood the school's TechSafe Policy.

- Users are provided with a school issued log-in username and password and are expected to keep them private.
- Students are not allowed to deliberately access online materials or files on the school network, of their peers, teachers or others.
- If you think your password may have been compromised or someone else has become aware of your password report this immediately to your classroom teacher, homeroom teacher, principal, and/or technology co-coordinators.
- All staff are aware of their individual responsibilities to protect the security and confidentiality of school server networks. They should also make certain that passwords are not shared and are changed periodically.

Managing the Internet

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it a resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. All use of internet is monitored by our web filter/content manager**.** All online and all network activity is logged and the logs are randomly but regularly monitored. Whenever any inappropriate use is detected it will be followed up.

- The school maintains students will have supervised access to Internet resources (where reasonable) through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with students.
- If Internet research is set for homework, it is advised that parents check the sites and supervise the work. Parents will be advised to supervise any further research.
- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources.

Infrastucture

- School internet access is controlled through the web and content filtering system.
- Staff and students are aware that school based email and internet activity is monitored and explored further if required.
- The school does not allow students access to internet logs.
- If staff or students discover an unsuitable or inappropriate site (including but not limited to images, text, sound, music or the like), the screen must be switched off/ closed and the incident reported immediately to the teacher and then to the TechSafe co-coordinators.
- It is the responsibility of the school, through contract agreement with ETA, to ensure that Anti-virus protection is installed on all school machines. This automatically updates.
- Students and staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility or ETA, to install or maintain virus protection on personal systems.
- Students and staff are not permitted to download programs or files on school owned technologies.
- If there are any issues related to viruses or anti-virus software, the Tech Safe co-coordinator should be informed. Contractual Preventive Maintenance Services are provided by ETA quarterly or as needed.
- All Grades 5 – 8 students, teachers, and principal have LanSchool downloaded on their device. LanSchool is a program which monitors the student computers when turned on. At all times the teacher will be able to see what each student in the class is doing on the computer. The principal has onscreen visualization to monitor all student computers at any time.

Mobile technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalized learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and Smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile devices (including cell phones)

- Per the Student Handbook, students are not allowed to use personal mobile devices during school hours unless special permission is given directly from a teacher or administration to a student.
- The school allows staff to bring in personal mobile phones and devices for their own use. Under certain circumstances the school allows a member of staff to contact a student or parent/ guardian using their personal device.
- Users bringing personal devices into school do so at their risk. The school is not responsible for the loss, damage or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the SJLS community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the SJLS community.
- Mobile phones are not provided to SJLS staff. They have their own.
- In certain circumstances (i.e. field trips, emergencies, weather, etc.), SJLS teachers would be required to keep their personal mobile device turned on and accessible at all times.
- Where the school provides a laptop and iPad for staff, only these devices may be used to conduct school business outside of school.

Managing email

The use of email within most schools is an essential means of communication for staff, students and families. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including; direct written contact between schools on different projects, staff based or student based, within school and beyond our school walls. We recognize that students need to understand how to style an email in relation to their age and good 'netiquette'.

- The school gives all staff their own email account and communication log-in information to use for all school business. This is to minimize the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- It is the responsibility of each account holder (stjohnsmayville.com) to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary email histories can be traced. This should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.
- The school requires a standard confidentially notice to be attached to all email correspondence, along with signature line of account holder. The responsibility for adding this disclaimer lies with the account holder.

- The following notice should be posted at the bottom of every email (including Forwards and Replies):

> *CONFIDENTIALITY NOTICE*
>
> *Note: This message and attachments are covered by the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, and contain information intended for the specified individual(s) only. This information is confidential. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify me immediately by replying to the message and deleting it from your computer. Thank you.*

- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. These will be through Google Apps for Education.
- All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Student must immediately tell a teacher/ trusted adult if they receive an offensive web communication.
- Staff must inform (the principal) if they receive an offensive web communication.
- Students in Grades 5 – 8 are introduced to email as part of the technology curriculum.

Safe Use of Images

Images, photographs, pictures and the like

Digital images are easy to capture, reproduce and publish and, therefore, at times may be misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking permission and considering the appropriateness.

- With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students for school and church related use.

Consent of adults who work at the school

- Permission to use images of all staff who work at the school is sought upon hire.

Publishing student's images and work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- on the school web site
- in the school's publications, including but not limited to school newsletters, year book, and informational brochures.
- in the school building on display boards
- other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcast
- in display material that may be used in the school's communal areas including the church
- in display material that may be used in external areas, ex. exhibition promoting the school
- general media appearances, ex. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, ex. divorce of parents, custody issues, etc.

Parents/guardians may withdraw permission, in writing, at any time. Consent has to be given by both parents/guardians in order for it to be deemed valid. Students' full names will not be published alongside their image and vice versa. E-mail, postal addresses and any other contact information of students will not be published. Students' full names will not be published.

Storage of Images

- Image files of children are stored on the school network server
- Rights of access to this material are restricted to the teaching staff and students within the confines of the school network.
- Technology co-coordinators have the responsibility of deleting the images when they are no longer required, or the student has left the school.

Webcams and video

- We do not use publicly accessible webcams in school
- Webcams in school are only used for specific learning and educational purposes, and never using images of children or adults.
- Misuse of the webcam and/or video of any member of the school community will result in sanctions

Video Conferencing

- Permission is sought from parents and guardians if their children are involved in video conferences (including in and outside of the school building)
- All students are supervised by a member of staff when video conferencing (including In and outside of the school building).
- Approval from administration is sought prior to all video conferences within school.
- No part of any video conference may be recorded in any medium without the written consent of all parties involved in the conference

Technology Issues and Troubleshooting

Comments and Complaints

Comments and complaints relating to this TechSafe policy and any technology in the school should be made directly to the technology co-coordinators and the administrator.

Record Keeping

All incidents in technology, malfunctions of digital equipment (laptops, iPads, Smartboards, etc.) will need to be reported to the administration who will log on flowcharts and make contact with who will solve the problem.
Some examples of incidences to report are:

- Printing issue
- Computer won't turn on
- Program not installed/won't open
- Wireless is not working

Please note that this record keeping is important for addressing and resolving computer issues on a timely basis and for long term technology planning and budgeting.

Immediate Technology Issues

Some incidences using technology do require immediate attention. If there is a technology issue in the classroom that prevents a student or teacher from completing a necessary task, contact one of the technology co-coordinators for troubleshooting suggestions. Some examples of these immediate problems may be:

- Cannot hook up Smartboard to computer to display lesson
- Unable to play a DVD
- As part of a lesson, software is not opening correctly or internet is not working
- Student Net Book problems

It is important to remember that some technology issues needing immediate attention may not be resolved immediately. When integrating technology for classroom lessons or use, it's vital that you take the time to try the technology ahead of time. As a general rule of thumb when using technology, try to have a back-up lesson in case technology issues cannot be resolved immediately.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the Technology co-coordinator and/or administration.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the technology co-coordinators, depending on the seriousness of the offence; investigation by the Administration, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences (see flowchart.)
- Users are made aware of sanctions relating to the misuse or misconduct on the Acceptable Use Agreement

Equal Opportunities

Pupils with additional needs

The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' TechSafe policy. However, teachers are aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of TechSafe issues.

Where a student has poor social understanding, careful consideration is given to group interactions when raising awareness of the TechSafe policy. Internet activities are planned and well managed for these children and young people.

Parental Involvement

- Parents, guardians and students are actively encouraged to contribute to the school TechSafe policy by letter and by reporting unsuitable sites, etc. to the TechSafe co-coordinators.
- Parents and guardians are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents and guardians are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (Ex: on school website)
- The school disseminates information to parents relating to TechSafe Policy where appropriate in the form of;
    - Website/Google postings
    - Newsletter items
    - Correspondence home

Writing and Reviewing this Policy

Review Procedure

There will be an on-going opportunity for staff to discuss with the technology co-coordinators any comments, concerns, revisions or suggestions they may have for the TechSafe Policy.

This policy will be reviewed every June by the Technology Vision Committee with recommendations from the SJLS staff. Consideration will be given to the implications for future whole school development planning.

This policy will be amended if new technologies are adopted or changed in any way.

Date approved by staff: ____________ **Date approved by Administration: ______________**

Signed: ____

Kay Koenitzer, Principal

Next review date: ________________________

St John’s Lutheran School Code of Conduct

Administration, Teachers, Staff and Visitors

School information communications technology and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of technology. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Principal.

Deliberate access to inappropriate materials by any user will lead to the incident being logged by the TechSafe Policy co-coordinators, depending on the seriousness of the offence; investigation by administration, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences

- I will only use the school’s email, network, internet and any related technologies for professional purposes or for uses deemed ‘reasonable’ by administration.
- I will comply with the network system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role and are done through school provided accounts (stjohnsmayville.com email)
- I will ensure that personal data (such as data and files saved in the server) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will not install any hardware or software without seeking permission from the technology co-coordinators.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional and educational purposes that align with school policy and with written consent of the parent, guardian or staff member. Images will not be distributed outside the school network without the permission of the parent/guardian, member of staff or administration.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to administration.
- I will respect copyright property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into jeopardy.
- I will support and promote the school’s TechSafe policy and help pupils to be safe and responsible in their use of information, communication and other related technologies.

User Signature
I agree to follow this code of conduct and to support the safe use of technology throughout St. John’s Lutheran School.

Signature____ Date____________

Full Name____ Job Title____________________

(Please Print)

St. John’s Lutheran School Student Acceptable Use Agreement

TechSafe Rules

- ✓ I understand that use of technology used for school purposes, both inside and out of the school building is an extension of the classroom. Any rules that apply within the classroom will apply to anything used online for school purposes.
- ✓ I will only use technology in school for school, learning and/or educational purposes.
- ✓ I will only open programs, websites, hardware and other technology sources my teacher approves.
- ✓ I will not tell other people my login information or any passwords.
- ✓ I will only open/delete my own files.
- ✓ I will make sure that all technology contact with other children and adults is responsible, respectful and Christian.
- ✓ I will not deliberately look for, save or send anything that could be unpleasant or inappropriate. If I accidentally find anything like this I will tell my teacher immediately.
- ✓ I will not give out my own personal information such as my name, phone number or home address. I will not arrange to meet someone.
- ✓ I will be responsible for my behavior when using technology because I know that these rules are made to keep me safe.
- ✓ I know that my use of technology (online, when using any computer, etc.) can be checked at any time and that my parent/guardian may be contacted if a member of school staff is concerned about my technology use or complying with this TechSafe policy.

S.M.I.L.E and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never give out this information online.

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or guardian and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, guardian, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, instant messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. Do not open or reply to messages from strangers.

St. John’s Lutheran School, 520 Bridge St., Mayville, WI 53050

Dear Parent,

School information communications technology including the use of internet has become an important part of learning in our school.   We expect all children to be safe and responsible when using any form of technology.

Please read and discuss these TechSafe rules with your child and return the slip at the bottom of this page to your classroom teacher. If you have any concerns or would like some explanation please contact our technology co-coordinators or our school principal, Kay Koenitzer.

- -✂- -

Parent/ Guardian signature

We have discussed this and ______________________________(child name) agrees to follow the TechSafe rules and to support the safe and responsible use of technology at St. John’s Lutheran School.

Parent/Guardian Signature

____

Grade ________Teacher ___________________________Date _______________

St. John’s Lutheran School, 520 Bridge St., Mayville, WI 53050

Dear Parent,

School information communications technology including the use of internet has become an important part of learning in our school.   We expect all children to be safe and responsible when using any form of technology.

Please read and discuss these TechSafe rules with your child and return the slip at the bottom of this page to your classroom teacher. If you have any concerns or would like some explanation please contact our technology co-coordinators or our school principal, Kay Koenitzer.

- -✂- -

Parent/ Guardian signature

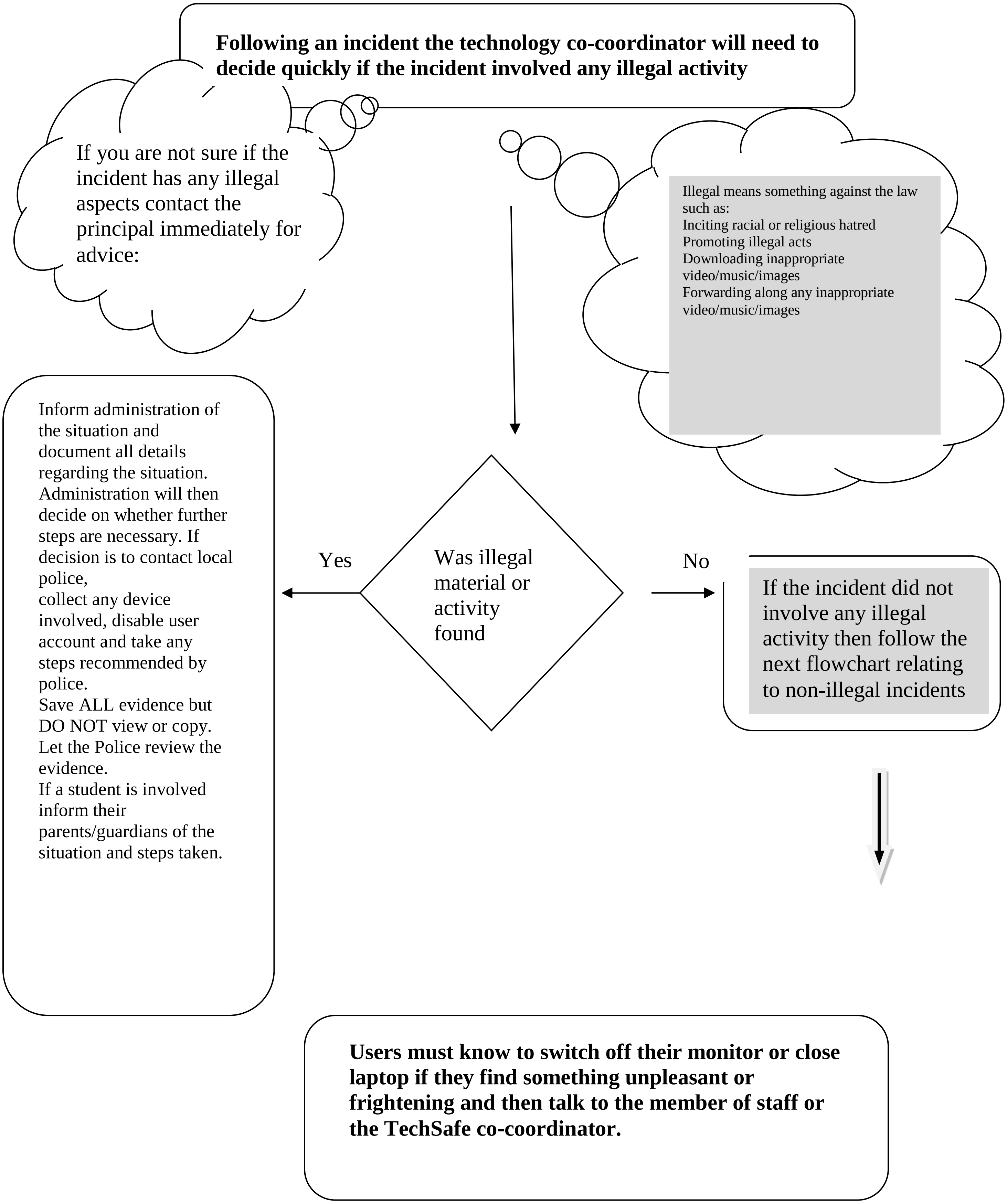
We have discussed this and ______________________________(child’s name) agrees to follow the TechSafe rules and to support the safe and responsible use of technology at St. John’s Lutheran School.

Parent/Guardian Signature

____

Grade ______Teacher ____________________________________Date ________

Flowchart for Managing a TechSafe Incident



Following an incident the technology co-coordinator will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact the principal immediately for advice:

Illegal means something against the law such as:
Inciting racial or religious hatred
Promoting illegal acts
Downloading inappropriate video/music/images
Forwarding along any inappropriate video/music/images

Was illegal material or activity found

Yes

Inform administration of the situation and document all details regarding the situation. Administration will then decide on whether further steps are necessary. If decision is to contact local police,
collect any device involved, disable user account and take any steps recommended by police.
Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.
If a student is involved inform their parents/guardians of the situation and steps taken.

No

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to the member of staff or the TechSafe co-coordinator.

Resources and References

http://cpsr.org/

http://kids.getnetwise.org/safetyguide/kids

http://www.kidsmart.org.uk/

http://www.isafe.org/

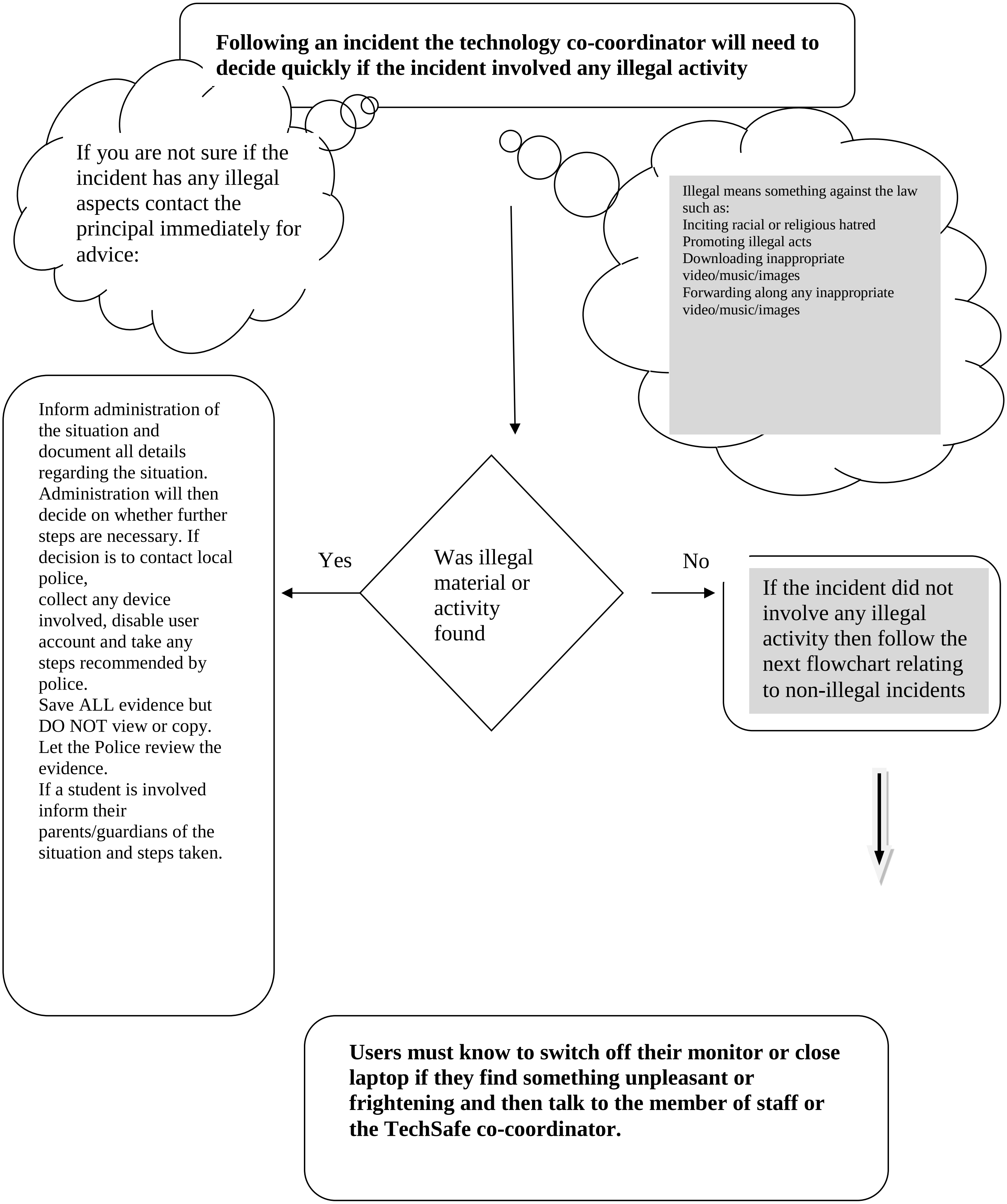
http://www.netsmartz.org/Safety/SafetyTips

St. John’s Lutheran School Technology Trouble Log

Details of ALL technology issues (including but not limited to: wireless not working, blue screen, doesn’t print, power on/off, unable to log-on, etc.) should be documented here. You will find this log located in the computer lab, both laptop carts and in the school office. Any issues may be recorded on any log as all are checked daily.

Date & Time	Name of pupil or staff	Computer #	Details of incident	Any actions or troubleshooting steps taken	Checked By

Flowchart for Managing a TechSafe Incident



Following an incident the technology co-coordinator will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact the principal immediately for advice:

Illegal means something against the law such as:
Inciting racial or religious hatred
Promoting illegal acts
Downloading inappropriate video/music/images
Forwarding along any inappropriate video/music/images

Was illegal material or activity found

Yes

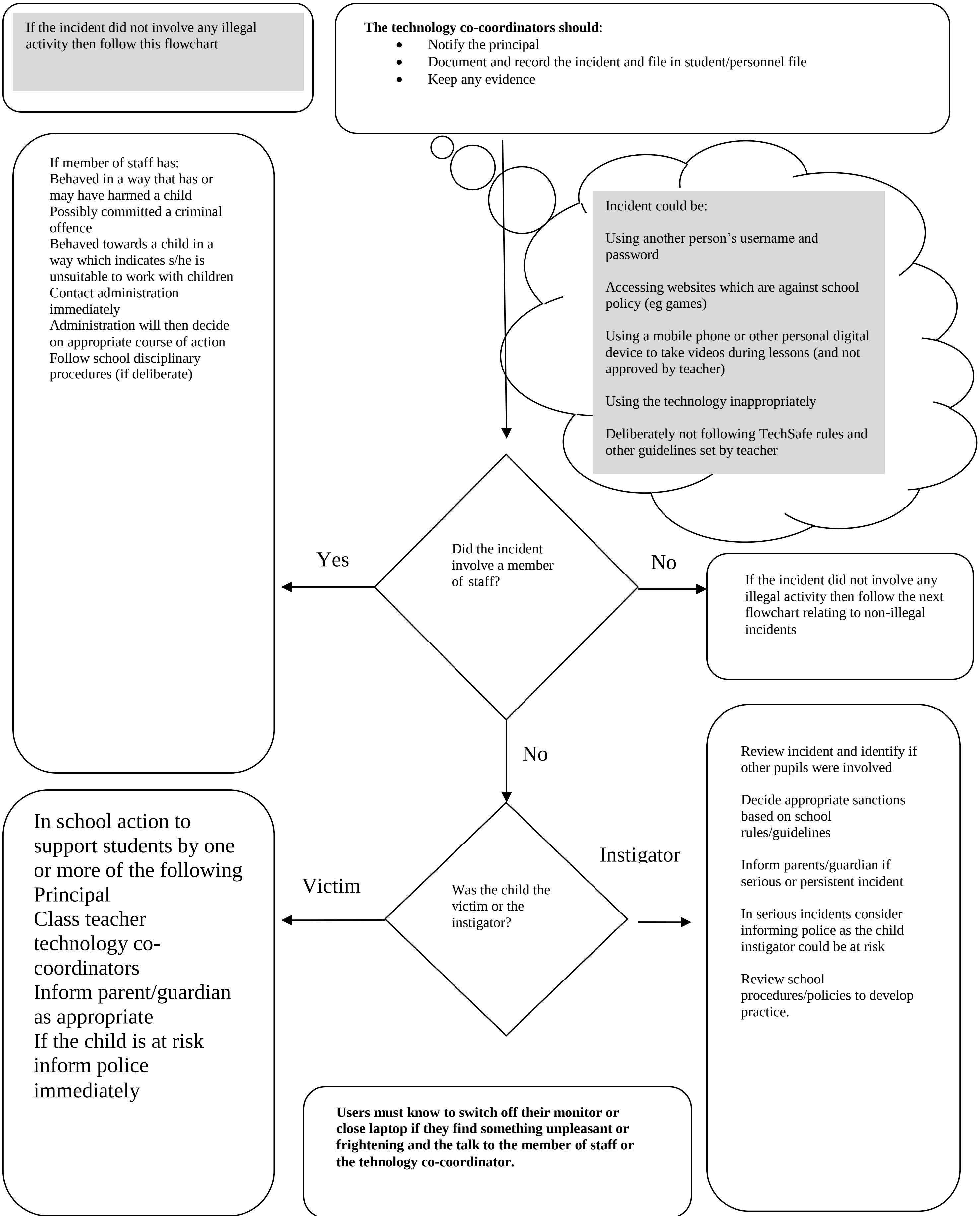
Inform administration of the situation and document all details regarding the situation. Administration will then decide on whether further steps are necessary. If decision is to contact local police,
collect any device involved, disable user account and take any steps recommended by police.
Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.
If a student is involved inform their parents/guardians of the situation and steps taken.

No

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to the member of staff or the TechSafe co-coordinator.

Flowchart for Managing a TechSafe Incident



If the incident did not involve any illegal activity then follow this flowchart

The technology co-coordinators should:

- Notify the principal
- Document and record the incident and file in student/personnel file
- Keep any evidence

Incident could be:

Using another person's username and password

Accessing websites which are against school policy (eg games)

Using a mobile phone or other personal digital device to take videos during lessons (and not approved by teacher)

Using the technology inappropriately

Deliberately not following TechSafe rules and other guidelines set by teacher

If member of staff has:
Behaved in a way that has or may have harmed a child
Possibly committed a criminal offence
Behaved towards a child in a way which indicates s/he is unsuitable to work with children
Contact administration immediately
Administration will then decide on appropriate course of action
Follow school disciplinary procedures (if deliberate)

Did the incident involve a member of staff?

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Was the child the victim or the instigator?

In school action to support students by one or more of the following
Principal
Class teacher
technology co-coordinators
Inform parent/guardian as appropriate
If the child is at risk inform police immediately

Review incident and identify if other pupils were involved

Decide appropriate sanctions based on school rules/guidelines

Inform parents/guardian if serious or persistent incident

In serious incidents consider informing police as the child instigator could be at risk

Review school procedures/policies to develop practice.

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and the talk to the member of staff or the tehnology co-coordinator.

Smile and Stay Safe Poster

E-Safety Rules to be displayed next to all PCs in school

S.M.I.L.E and Stay Safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never give out this information online.

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or guardian and they can be with you.

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, guardian, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online.

Emails, downloads, instant messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. Do not open or reply to messages from strangers.

Resources and References

http://cpsr.org/

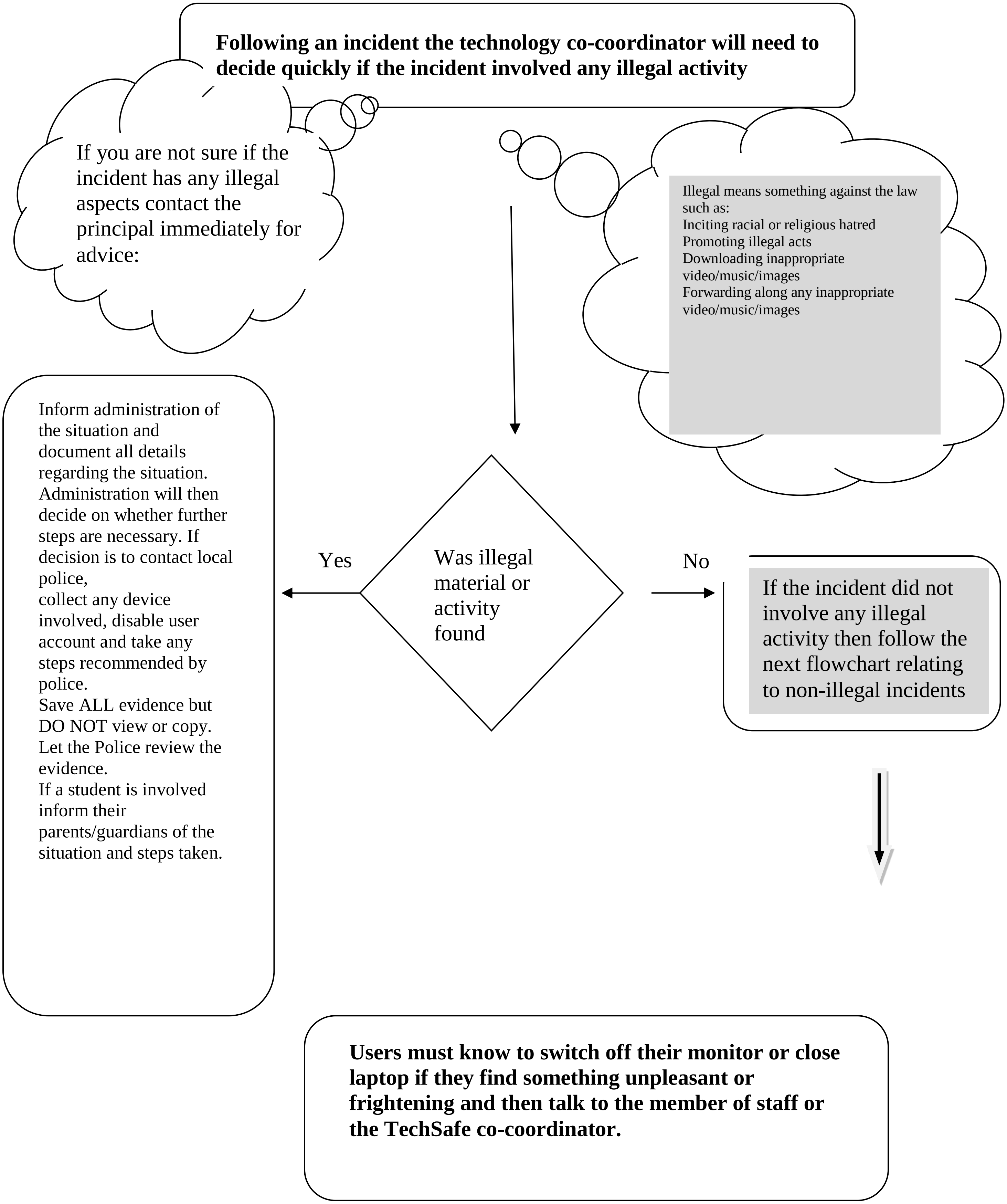
http://kids.getnetwise.org/safetyguide/kids

http://www.kidsmart.org.uk/

http://www.isafe.org/

http://www.netsmartz.org/Safety/SafetyTips

Flowchart for Managing a TechSafe Incident



Following an incident the technology co-coordinator will need to decide quickly if the incident involved any illegal activity

If you are not sure if the incident has any illegal aspects contact the principal immediately for advice:

Illegal means something against the law such as:
Inciting racial or religious hatred
Promoting illegal acts
Downloading inappropriate video/music/images
Forwarding along any inappropriate video/music/images

Was illegal material or activity found

Yes

Inform administration of the situation and document all details regarding the situation. Administration will then decide on whether further steps are necessary. If decision is to contact local police,
collect any device involved, disable user account and take any steps recommended by police.
Save ALL evidence but DO NOT view or copy. Let the Police review the evidence.
If a student is involved inform their parents/guardians of the situation and steps taken.

No

If the incident did not involve any illegal activity then follow the next flowchart relating to non-illegal incidents

Users must know to switch off their monitor or close laptop if they find something unpleasant or frightening and then talk to the member of staff or the TechSafe co-coordinator.