St John’s School (SCE)
Acceptable use policy and Guidance

1. What is an AUP (Acceptable Use Policy)?

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all on-line technologies (including the Internet, E-mail, web cams, Instant Messaging and other social networking spaces, mobile phones and games) to safeguard adults and children and young people within the school setting. It details how the school will provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies, beyond the school setting. It also explains procedures for any unacceptable or misuse of these technologies by adults or children and young people.

2. Why have an AUP?

The use of the Internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain therefore it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children use these technologies. These risks include:

- Commercial issues with spam and other inappropriate e-mail.
- Grooming by predators, usually pretending to be someone younger than their true age.
- Illegal activities of downloading or copying any copyright materials and file-sharing via the Internet or any mobile device.
- Viruses.
- Cyber-bullying.
- On-line content which is abusive or pornographic.

BECTA defines these as the three Cs being commerce, content and contact.

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks. This also includes online forums, blogs, wikis etc which must be hosted via the Virtual Learning Environment section of the school web page.

Whilst the school acknowledges that we will endeavour to safeguard against all risks we may never be able to completely eliminate them. Any incidents that may arise will be dealt with quickly and according to policy to ensure children and young people are continued to be protected.

As part of the Every Child Matters agenda set out by the government, the Education Act 2002 and the Children’s Act 2004, it is the duty of schools to ensure that children and young people are protected from potential harm both within and beyond the school environment. Therefore, the involvement of children and young people and parent/carers is also vital to the successful use of on-line technologies, so this policy also aims to inform how parents/carers and children or young people are part of the procedures and how children and young people are educated to be safe and responsible users so that they can make good judgements about what they see, find and use. The term ‘e-safety’ is used to encompass the safe use of all on-line technologies in order to protect children, young people and adults from potential and known risks.

3. Aims

- To ensure the safeguarding of all adults, children and young people within and beyond the school setting by detailing appropriate and acceptable use of all on-line technologies.
- To outline the roles and responsibilities of everyone.
- To ensure adults are clear about procedures for misuse of any on-line technologies both within and beyond the school setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of benefits and potential issues of on-line technologies.

4. Roles and responsibilities of the school:

4.1 Headteacher

It is the overall responsibility of the Headteacher to ensure that there is an overview of e-Safety (as part of the wider remit of Child Protection) across the school with further responsibilities as follows:

- The Headteacher has designated an e-Safety Leader to implement agreed policies, procedures, staff training, curriculum requirements and take the lead responsibility for ensuring e-Safety is addressed in order to establish a safe ICT learning environment.
- Time and resources will be provided for the e-Safety Leader and staff to be trained and update policies, where appropriate.
- The Headteacher is responsible for promoting e-Safety across the curriculum and has an awareness of how this is being developed, linked with the school development plan.
- The Headteacher will inform the SGC at the Curriculum meetings about the progress of or any updates to the e-Safety curriculum (via PSHE or ICT) and ensure SGC members know how this relates to child protection. At SGC meetings, all members will be made aware of e-Safety developments from the Curriculum meetings.

4.2 e-Safety Leader

It is the role of the designated e-Safety Leader to:

- Ensure that the AUP is reviewed annually, with up-to-date information available for all staff to teach e-Safety and for parents to feel informed and know where to go for advice.
- Ensure that filtering is set to the correct level for staff and children and young people, in the initial set up of a network, stand-a-lone PC, staff/children laptops and the learning platform by ensuring the technician is informed and carries out work as directed.
- Ensure that all adults are aware of the filtering levels and why they are there to protect children and young people.
- Report issues and update the Headteacher on a regular basis.
- Liaise with the PSHE, Child Protection and ICT leads so that policies and procedures are up-to-date to take account of any emerging issues and technologies.
- Update staff training (all staff) according to new and emerging technologies so that the correct e-safety information can be taught or adhered to.
- Ensure that the network manager has in place monitoring protocols for the school network and other on-line technologies such as staff email.
- The use of personal equipment in school or settings for work purposes, such as a digital camera and digital recorders are not recommended.
- The use of school equipment at home excluding laptops should be with the written agreement of the asset holder
- The Network Manager ensures there is appropriate and up-to-date anti-virus software and anti-spyware on the network, stand-a-lone PCs and teacher/child laptops and other online devices and that this is reviewed and updated on a regular basis.
- Ensure that staff can check for viruses on laptops, stand-a-lone PCs and memory sticks or other transferable data files to minimise issues of virus transfer.

4.3 Staff

It is the responsibility of all adults within the school to:

- Ensure that they know who the named person for Child Protection is within school so that any misuse or incidents can be reported which involve a child. Where an allegation is made against a member of staff it should be reported immediately to the Headteacher.
- Be familiar with the Behaviour, Anti-bullying and other relevant policies so that in the event of misuse or an allegation, the correct procedures can be followed, immediately. In the event that a procedure is unknown, they will refer to the Headteacher immediately.
- Check the filtering levels are appropriate for their children and young people and are set at the correct level *(all staff have undergone an e-safety awareness briefing)*. Report any concerns to the E-safety Leader.

- Alert the e-Safety Leader of any new or arising issues and risks that may need to be included within policies and procedures.
- Ensure that children and young people are protected and supported in their use of on-line technologies so that they know how to use them in a safe and responsible manner so that they can be in control and know what to do in the event of an incident.
- Be up-to-date with e-Safety knowledge that is appropriate for the age group and reinforce through the curriculum.
- Use electronic communications in an appropriate way that does not breach the Data Protection Act 1998.
  Remember confidentiality and not disclose information from the network, pass on security passwords or leave a station unattended when they or another user is logged in.
- Ensure that they follow the correct procedures for any data required to be taken from the school premises.
- Report accidental access to inappropriate materials to the e-Safety Leader, ICT Coordinator and/or the network manager in order that inappropriate sites are added to the restricted list.
- Use anti-virus software and check for viruses on their work laptop, memory stick or a CD ROM when transferring information from the Internet on a regular basis, especially when not connected to the school network.
- Report incidents of personally directed "cyber bullying" or other inappropriate behaviour via the Internet or other technologies using the accident/incident reporting procedure in the same way as for other non-physical assaults.

4.4 Children and young people

Children and young people are:

- Involved in the review of our Acceptable Use Rules through the school council or other appropriate group, in line with this policy being reviewed and updated.
- Responsible for following the Acceptable Use Rules whilst within school as agreed at the beginning of each academic year or whenever a new child attends the school or setting for the first time. This also applies to the use of the virtual learning section of the school website outside of school.
- Taught to use the Internet in a safe and responsible manner through ICT, PSHE or other clubs and groups.
- Taught to tell an adult about any inappropriate materials or contact from someone they do not know straight away, without fear of reprimand (age and activity dependent).

4. Appropriate use by staff or adults

Staff members have access to the network so that they can access age appropriate resources for their classes and create folders for saving and managing resources.
They have a password to access a filtered Internet service and know that this should not be disclosed to anyone or leave a computer or other device unattended whilst they are logged in.

All staff will receive a copy of the Acceptable Use Policy and a copy of the Acceptable Use Rules, which then need to be signed, returned to school or setting to keep under file with a signed copy returned to the member of staff.

The Acceptable Use Rules are displayed in the staff room as a reminder that staff members need to safeguard against potential allegations and a copy of this policy is provided to all staff for home use.

When accessing the VLE area of the web page from home, the same Acceptable Use Rules will apply.

5.1 In the event of inappropriate use

If a member of staff is believed to misuse the Internet or learning platform in an abusive or illegal manner, a report must be made to the Headteacher immediately and then the Allegations against staff Procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities contacted.

Allegations are defined as information relating to either potential criminal conduct or conduct raising concerns about a person's suitability.

In the lesser event of misuse or accidental misuse refer to appendices for a list of actions relating to the scale of misuse.

5. Appropriate use by children and young people

Acceptable Use Rules and the letter for children and young people and parents/carers are outlined in the Appendices and detail how children and young people are expected to use the Internet and other technologies within school or other settings, which includes downloading or printing of any materials. The rules are there for children and young people to understand what is expected of their behaviour and attitude when using the Internet which then enables them to take responsibility for their own actions. For example, knowing what is polite to write in an e-mail to another child or understanding what action to take should there be the rare occurrence of sighting unsuitable material. This also includes the deliberate searching for inappropriate materials and the consequences for doing so.

The rules should be displayed prominently within the classrooms and in the computer suite.

We want our parents/carers to support our rules with their child or young person, which is shown by signing the Acceptable Use Rules together so that it is clear to the school or setting, the rules are accepted by the child or young person with the support of the parent/carer. This is also intended to provide support and information to parents/carers when children and young people may be using the Internet beyond school.

The downloading of materials, for example, music files and photographs need to be appropriate and 'fit for purpose' based on research for work and be copyright free.

File-sharing via e-mail, weblogs or any other means on-line should be appropriate and be copyright free when using the VLE section of the web page in or beyond school.

6.1 In the event of inappropriate use

Should a pupil be found to misuse the on-line facilities whilst at school, through the web page or in a setting beyond the school, then consequences consistent with the school's disciplinary systems will occur. For example:

- Any child found to be wilfully misusing the Internet by not following the Acceptable Use Rules will have a letter sent home to parents/carers explaining the reason for suspending the child or young person's use for a particular lesson or activity.
- Further misuse of the rules will result in not being allowed to access the Internet for a period of time and another letter will be sent home to parents/carers.
- A letter will be sent to parents/carers outlining the breach in Child Protection Policy where a child or young person is deemed to have misused technology against another child or adult.
- Access to the electronic resources could ultimately be removed if persistent misuse occurs.

In the event that a child or young person **accidentally** accesses inappropriate materials the child should report this to an adult immediately and take appropriate action to hide the screen or close the window, e.g. use 'Hector Protector', for example, (dependent on age) so that an adult can take the appropriate action. Where a child or young person feels unable to disclose abuse, sexual requests or other misuses against them to an adult, they can use the Report Abuse button (www.thinkuknow.co.uk) to make a report and seek further advice. The issue of a child or young person deliberately misusing on-line technologies should also be addressed by the school in a manner consistent with it's disciplinary procedures.

Children should also be taught and encouraged to consider the implications for misusing the Internet and posting inappropriate materials to websites, for example, as this can lead to legal implications.

7. The curriculum and tools for Learning

7.1 Internet use

We teach our pupils how to use the Internet safely and responsibly, for researching information, exploring concepts, deepening knowledge and understanding and communicating effectively in order to further learning, through ICT and/or PSHE lessons where the following concepts, skills and competencies have been taught by the time they leave school:

- Internet literacy
- making good judgements about websites and e-mails received
- knowledge of risks such as viruses and opening mail from a stranger
- access to resources that outline how to be safe and responsible when using any on-line technologies
- knowledge of copyright and plagiarism issues (Secondary)
- file-sharing and downloading illegal content
- uploading information – know what is safe to upload and not upload personal information
- where to go for advice and how to report abuse.

The revised framework for key stage three ICT and functional skills ICT requires young people to learn e-Safety as part of their continuing education schools will need to explain how they are addressing the needs of this aspect of the curriculum, e.g. Most pupils recognise the need to be safe and act responsibly when using digital communications.

These skills and competencies are taught within the curriculum so that children and young people have the security to explore how on-line technologies can be used effectively, but in a safe and responsible manner. Children and young people will know how to deal with any incidents with confidence, as we adopt the 'never blame the child for accidentally accessing inappropriate materials' culture, in the event that they have **accidentally** accessed something.

Personal safety – ensuring information uploaded to web sites and e-mailed to other people does not include any personal information including:

- full name (first name is acceptable, without a photograph)
- address
- telephone number
- home e-mail address
- school
- clubs attended and where
- age or DOB
- names of parents
- routes to and from school
- identifying information, e.g. I am number 8 in the Youth Football Team

Photographs should only be uploaded on the approval of a member of staff or parent/carer and should only contain something that is appropriate in line with SCE policy'. Parents/carers should monitor the content of photographs uploaded. Images of children and young people should be stored according to policy.

7.2 E-mail use

The school provides each student with an e-mail addresses to use, as a class and/or as individuals as part of their entitlement to being able to understand different ways of communicating and using ICT to share and present information in different forms.

It is important that students and staff use their school email accounts for all school matters as these accounts are monitored and tracked, by appropriate software, to ensure appropriate use.

7.3 Video-conferencing

The use of video-conferencing equipment will be via the schools internet connection which is a filtered service. Students should not access this facility unless a member of staff is present.
Students should alert a member of staff immediately of any inappropriate use by another child or adult. (This is part of the Acceptable Use Rules.)

Where children and young people (and adults) may be using a web cam in a family area at home, they should have open communications with parents/carers about their use and adhere to the Acceptable Use Rules.

7.4 Mobile phones and other technologies

The use of mobile phones and other portable devices such as MP3 players is not allowed in our school. If a students brings such a device into school this will be dealt with in line with existing disciplinary procedures.

Staff must not use their personal numbers to contact pupils under any circumstances.

7.5 Video and photographs

The term 'image' refers to the taking of video footage or photographs via any camera or other technology, e.g. a mobile phone. When in school there is access to:
**need to list access to camera and web cam equipment in school*

The sharing of photographs via weblogs, forums or any other means on-line will only occur after permission has been given by a parent/carer or member of staff.

Any photographs or video clips uploaded should not have a file name of a child, especially where these may be uploaded to a school website. Photographs should only ever include the child's first name although Child Protection Guidance states either a child's name or a photograph but not both. Group photographs are preferable to individual children and young people and should not be of any compromising positions or in inappropriate clothing, e.g. certain types of gym kit.

8. Filtering and safeguarding measures

Staff, children and young people are required to use their network area and all tools within it, in an acceptable way.

9. Monitoring

The use of on-line technologies and /or the school network by children, young people and staff, is monitored on a regular basis.

10. School library and other study areas

The computers in the school library, and other study areas, are protected in line with the school network.

Where software is used that requires a child login, it is password protected so that the child is only able to access themselves as a user. All students are taught not to share passwords.
The same acceptable use rules apply for any staff and children and young people using this technology.

11. Parents

11.1 Roles

(There is no statutory requirement for parents to sign acceptable use policies but evidence shows that children and young people signing agreements to take responsibility for their own actions, is successful. http://www.teachers.tv/video/22517 shows an excellent example of this for bullying.)

Each child or young person will receive a copy of the Acceptable Use Rules on an annual basis or first-time entry to the school which need to be read with the parent/carer, signed and returned to school confirming both an understanding and acceptance of the rules *(as part of induction procedure).*

It is expected that parents/carers will explain and discuss the rules with their child, where appropriate, so that they are clearly understood and accepted.

School will keep a record of the signed forms.

11.2 Support

Schools and settings may choose to follow or adapt this guidance:
As part of the approach to developing e-safety awareness with children and young people, the school offers parents the opportunity to find out more about how they can support the school in keeping their child safe and find out what they can do to continue to keep them safe whilst using on-line technologies beyond school, this is done via parental briefings and parents fact sheets. The school aims to promote a positive attitude to using the internet and therefore wanst parents to support their child's learning and understanding of how to use on-line technologies safely and responsibly.
We will hold Parent/Carer Information training once per annum and use the Childnet International 'KnowITAll for Parents' CD/on-line materials (http://www.childnet-int.org.uk/kia/parents/cd/) to deliver key messages and raise awareness for parents/carers and the community

12. Links to other policies

12.1 Behaviour and Anti-Bullying Policies

Please refer to the Behaviour Policy for the procedures in dealing with any potential bullying incidents via any on-line communication, such as mobile phones, e-mail or blogs. Schools should have an up to date Anti-bullying Policy which will include any cyberbullying issues.

As a school we not treat on-line behaviours differently to off-line behaviours and we have exactly the same expectations for appropriate behaviour.

12.2 Allegation Procedures and the Child Protection Policy

Please refer to the Allegations against staff Procedure, Section 12, in order to deal with any incidents that occur as a result of using personal mobile or e-mail technologies which may result in an allegation of misuse or misconduct being made by any member of staff or child about a member of staff.

Allegations should be reported to the Headteacher immediately or to the named designated officers in HQ SCE in line with the allegations against staff procedure.

The DCSF White Paper clearly states that no personal equipment belonging to staff should be used when contacting children and young people and young people about homework or any other school issues either in or beyond school and any such action should be dealt with. We follow this information to protect our staff members from potential allegations of misconduct by a child or parent.

12.3 PSHE

We link the teaching and learning of e-Safety with our PSHE curriculum by ensuring that the key safety messages are the same whether children and young people are on or off line engaging with other people.

12.4 Health and Safety

Refer to the Health and Safety Policy and procedures of the school/setting and the Agency for information on related topics, particularly Display Screen Equipment, Home working and Accident/Incident reporting procedures. Wireless technologies are not considered to be a hazard following advice from the Health Protection Agency to the Government.

12.5 School website

The uploading of images to the school website will be subject to the same acceptable rules as uploading to any personal on-line space. Permission is always sought from the parent/carer prior to the uploading of any images. Settings should consider which information is relevant to share with the general public on a website and use secure areas for information pertaining to specific audiences.

12.6 External websites

In the event that a member of staff finds themselves or another adult on an external website, such as ‘Rate My Teacher’, as a victim, schools/settings are encouraged to report incidents to the Headteacher and unions, using the reporting procedures for monitoring.

Appendices

Staff Procedures Following Misuse by Children and Young People

The Headteacher will ensure that these procedures are followed, in the event of any misuse of the Internet, by a child or young person:

A. An inappropriate website is accessed inadvertently:
Reassure the child that they are not to blame and praise for being safe and responsible by telling an adult.
Report website to the e-Safety Leader if this is deemed necessary.
Contact the helpdesk service so that it can be added to the banned list.
Check the filter level is at the appropriate level for staff use in school.

B. An inappropriate website is accessed deliberately:
Refer the child to the Acceptable Use Rules that were agreed.
Reinforce the knowledge that it is illegal to access certain images and police can be informed.
Decide on appropriate sanction.
Notify the parent/carer.
Inform Agency as above.

C. An adult or child has communicated with a child or used ICT equipment inappropriately:
Ensure the child is reassured and remove them from the situation immediately.
Report to the Headteacher and Named person for Child Protection immediately.
Preserve the information received by the child if possible and determine whether the information received is abusive, threatening or innocent.
If illegal or inappropriate misuse the Headteacher must follow the existing child protection procedures
Contact CEOP (police) as necessary.

D. Threatening or malicious comments are posted to the school website or learning platform about a child in school:
Preserve any evidence.
Inform the Headteacher immediately.
Inform the Agency and e-Safety Leader so that new risks can be identified.
Contact the police or CEOP as necessary.

E. Threatening or malicious comments are posted on external websites about an adult in the school or setting:
Preserve any evidence.
Inform the Headteacher immediately.

N.B. There are three incidences when you must report directly to the police.

- Indecent images of children found.
- Incidents of 'grooming' behaviour.
- The sending of obscene materials to a child.

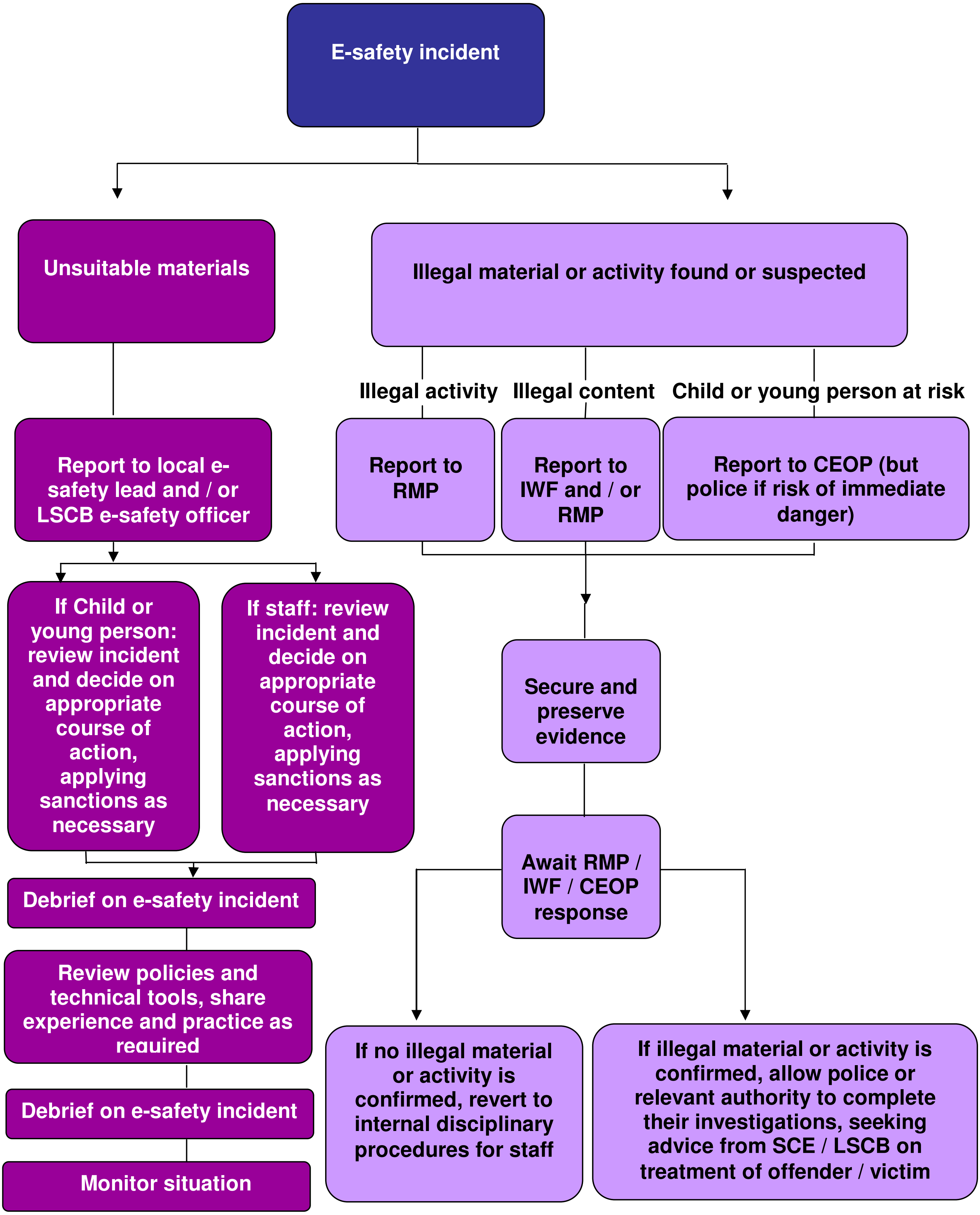
CEOP advice is to turn off the screen, secure the machine and contact the police for further instructions if an indecent image is found.
They will advise on how to deal with the machine, if they are unable to send out a forensics team immediately.
If in doubt, do not power down the machine.

Grabbing a screenshot is not a technical offence of distribution, but of 'making' an image.

- www.iwf.org.uk will provide further support and advice in dealing with offensive images on-line.

It is important to remember that any offensive images that may be received should never be forwarded to anyone else, even if it is to report them as illegal as this constitutes illegal activity and you will be liable to prosecution and investigation by the police.

Flowchart for responding to e-safety incidents


E-safety incident
Unsuitable materials
Illegal material or activity found or suspected
Illegal activity
Illegal content
Child or young person at risk
Report to local e-safety lead and / or LSCB e-safety officer
Report to RMP
Report to IWF and / or RMP
Report to CEOP (but police if risk of immediate danger)
If Child or young person: review incident and decide on appropriate course of action, applying sanctions as necessary
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Secure and preserve evidence
Await RMP / IWF / CEOP response
Debrief on e-safety incident
Review policies and technical tools, share experience and practice as required
Debrief on e-safety incident
Monitor situation
If no illegal material or activity is confirmed, revert to internal disciplinary procedures for staff
If illegal material or activity is confirmed, allow police or relevant authority to complete their investigations, seeking advice from SCE / LSCB on treatment of offender / victim

e-Safety Acceptable Use Rules Letter to Parents/Carer

Dear Parent/Carer,

As part of an enriched curriculum your child will be accessing the Internet, E-mail and personal on-line space via the Virtual Learning section of the school web site.

In order to support the school in educating your child about e-Safety (safe use of the Internet), please read the following Rules with your child then sign and return the slip.

In the event of a breach of the Rules by any student in the school, the e-Safety Policy lists further actions and consequences, should you wish to view it.

These Rules provide an opportunity for further conversations between you and your child about safe and appropriate use of the Internet and other on-line tools (e.g. mobile phone), both within and beyond school (e.g. at a friend's house or at home).

Should you wish to discuss the matter further please contact me at the school.

Yours faithfully,

Me!

....

e-Safety Acceptable Use Rules Return Slip

Child Agreement:

Name: __________________________________Class:__________________________

- I understand the Rules for using the Internet, E-mail and on-line tools, safely and responsibly.
- I know that the adults working with me at school will help me to stay safe and check that I am using the computers to help me with my work.

Child Signature: _____________________________________ Date: _______________

Parent/Carer Agreement:

- I have read and discussed the Rules with my child and confirm that he/she has understood what the Rules mean.
- I understand that the school will use appropriate filtering and ensure appropriate supervision when using the Internet, E-mail and on-line tools. I understand that occasionally, inappropriate materials may be accessed and accept that the school will endeavour to deal with any incident that may arise, according to policy.
- I understand that whilst my child is using the Internet and other on-line tools outside of school, that it is my responsibility to ensure safe and responsible use with the support of the school.

Parent/Carer Signature: ______________________________ Date: ________________

Secondary e- Safety awareness for students

We are encouraged to use and be aware of the safety rules and procedures which regulate our use of the ICT resources, including the Internet. At St John's School, we are encouraged and allowed to access our curriculum network and the Internet, enabling us to use vast resources and communicate, in support of research and education.

We insist that these facilities are used for educational purposes and in an appropriate manner. We are responsible for our behaviour and communication. We know that any breach of the rules will be considered a disciplinary matter and we agree to the following rules:

- **We know access to the networked resources is our privilege. We are encouraged to make use of the Internet in support of our studies in all subjects.**
- **We need to make sure we are supervised when we use the Internet at school or at home.**
- **We do not access, create or display any material (images, sounds, text, and video) which is likely to cause offence, inconvenience or anxiety to ourselves and others.**
- **We follow our teacher's instructions carefully.**
- **We must have permission from our parents/carers before we can use the Internet for our own independent research at school.**
- **We ask "Is it true?" We do not assume that information published on the Web or written in an e-mail is accurate or true.**
- **We keep our username and password private. We do not tell anyone.**
- **When we use e-mail, we only write to people we know in person or mentors approved by our teacher in school.**
- **We are careful about what we write. We check our work before we print or send anything. We do not use bad language. We do not write racist, sexist, abusive, homophobic or aggressive words. We do not write things that could upset and offend others. We could give ourselves and the school a bad name.**
- **We do not ever give personal information about ourselves and anyone else, such as our address, telephone number and private details in an e-mail or on a Website. We know we could put ourselves or others in danger.**
- **We do not respond to bad e-mail messages. We let our teachers know immediately if we are sent anything we do not feel comfortable with.**
- **We are wise net surfers. We do not go to sites or download any materials, which are offensive, violent and pornographic.**
- **We always respect the privacy of other users' files.**
- **We will report any incident that breaches the Acceptable Use Policy rules immediately to our teacher.**
- **We know that we can go to www.thinkuknow.co.uk for help.**

Further Information and Guidance

The nature of e-safety is evolving. You may want to keep up to date with further supporting documents, information or advice, which can be found on:

- www.parentscentre.gov.uk (for parents/carers)
- www.ceop.co.uk (for parents/carers and adults)
- www.iwf.org.uk (for reporting of illegal images or content)
- www.thinkuknow.co.uk (for all children and young people with a section for parents/carers and adults – this also links with the CEOP (Child Exploitation and On-line Protection Centre work)
- www.netsmartzkids.org (5 – 17)
- www.kidsmart.org.uk – (all under 11)
- www.phonebrain.org.uk (for Yr 5 – 8)
- www.bbc.co.uk/cbbc/help/safesurfing (for Yr 3/4)
- www.hectorsworld.com (for FS, Yr 1 and 2 and is part of the thinkuknow website above)
- www.teachernet.gov.uk (for schools and settings)
- www.dcsf.gov.uk (for adults)
- www.digizen.org.uk (for materials from DCSF around the issue of cyberbullying)
- www.becta.org.uk (advice for settings to update policies) and http://www.nextgenerationlearning.org.uk/esafetyandwifi.html (simple tips for parents/adults)
- www.nen.org.uk (for schools and settings – access to the National Education Network)