St Joseph's College
E-Safety Policy

Date Reviewed- September 2021

Next Review Date- September 2022

Chair of Governor's signature: 

Policy Statement

For clarity, the E-Safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. Parent/Carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – students, all staff, governing body, parents, volunteers.

Safeguarding is a serious matter; at St. Joseph's College we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as E-Safety is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an E-Safety incident, whichever is sooner.

The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the student or liability to the school.

This policy is available for anybody to read on the St Joseph's College website; upon review all members of staff will sign as read and understood both the E-Safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Student Use of ICT Agreement will be sent home with students at the beginning of each school year with a permission slip. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Governing Body

The Governing Body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any E-Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure E-Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.

- Appoint one governor to have overall responsibility for the governance of E-Safety at the school who will:

    - Keep up to date with emerging risks and threats through technology use.
    - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
    - Chair the Student Wellbeing Committee.

Headteacher
Reporting to the Governing Body, the Headteacher has overall responsibility for E-Safety within our school. The day-to-day management of this will be delegated to a member of staff, the E-Safety Officer, as indicated below.

The Headteacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. students, all staff, senior leadership team and governing body, parents.
- All E-Safety incidents are dealt with promptly and appropriately.

Designated Safeguarding Lead (E-Safety Officer)

The day-to-day duty of E-Safety is devolved to Mr. G Mantillas (Deputy Headteacher)

The E-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, Governing Body on all E-Safety matters.
- Engage with parents and the school community on E-Safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the E-Safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

ICT Technical Support Staff

Technical support staff are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any E-Safety technical solutions such as Internet filtering are operating correctly.
    - Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the E-Safety officer and Headteacher.
    - Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 8 characters.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any E-Safety incident is reported to the Head of Year or E-Safety Officer (and an E-Safety Incident report is made), or in his/her absence to the Headteacher. If you are unsure the matter is to be raised with the E-Safety Officer or the Headteacher to make a decision.

All Students

The boundaries of use of ICT equipment and services in this school are given in the student Use of ICT Agreement; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the behaviour policy.

E-Safety is embedded into our curriculum; students will be given the appropriate advice and guidance by staff. Similarly all students will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents and Carers

Parents play the most important role in the development of their children; as such the school will ensure that parents have the skills and knowledge they need to ensure the safety of children outside the school environment. Through parent's evenings, school newsletters, parent mail, the school will keep parents up to date with new and emerging E-Safety risks, and will involve parents in strategies to ensure that students are empowered.

Parents must also understand the school needs have to rules in place to ensure that their child can be properly safeguarded. As such parents will sign the student Acceptable Use Policy before any access can be granted to school ICT equipment or services.

Technology

St. Joseph's College uses a range of devices including PC, laptop, Apple Mac, iPad. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use Smoothwall software that prevents unauthorized access to illegal websites. It also prevents access to inappropriate websites; appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. The ICT Coordinator, E-Safety Officer and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

Email Filtering – we use Sofos Pure Message software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Passwords – all staff and students will be unable to access any device without a unique username and password.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as key drives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this E-Safety and the staff Acceptable Use Policy; students upon signing and returning their acceptance of the Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.
Students are permitted to use the school email system, and as such will be given their own email address.

Photos and videos – All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – There are many social networking services available; St. Joseph's College is fully supportive of social networking as a tool to engage and collaborate with learners, and to engage with parents and the wider school community.

In addition, the following is to be strictly adhered to:

- Permission slips (via the school photographic policy) must be consulted before any image or video of any child is uploaded.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a Licence which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Incidents - Any E-Safety incident is to be brought to the immediate attention of the E-Safety Officer, or in his/her absence the Headteacher. The E-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Training and Curriculum - It is important that the wider school community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues. As such, St. Joseph's College will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the student's learning.

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The E-Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

St. Joseph's College
ICT Acceptable Use Policy
Staff Guidelines

The School provides computers for use by staff, offering access to Management Information Systems, curriculum software and the Internet. The systems have great potential to support teaching and learning as well as CPD. The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources and help to ensure they remain available to all.

Equipment

- Do not install, attempt to install or store programs of any type on network computers.
- Do not attempt to change the configuration of the computer or add/remove printers or other Hardware.
- Computers should be used for educational purposes. Activities such as buying or selling goods are inappropriate as is also use of gambling websites.
- Always check files brought in on removable media (such as, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Ensure that you have antivirus updates installed on mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) and that they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from ICT equipment.

Classroom and Interactive Board Use

- Staff are responsible for ensuring projectors are turned off when vacating the classroom.
- Where ICT facilities are shared, there is the expectation that the equipment is left in a condition so that he next member of staff may use it effectively. Items which are lost or damaged must be reported immediately to ICT support.

Security and Privacy

- Individuals using a computer must log off when leaving the computer unattended unless it is only left unattended for a short period of time in which case it must be locked.
- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Senior Leadership Team (SLT) reserves the right to ask ICT staff to review your files and communications to ensure that you are using the system responsibly and appropriately.
- Whenever possible, confidential or sensitive data should not be saved to a local hard drive or portable device. If it is necessary to save confidential files to a local hard drive e.g. when working on a laptop away from school, they should be transferred to a network drive at the earliest opportunity and the local copy deleted.

Internet

- You should access the Internet only for school-based activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display. Transmission or gaining access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not use Instant Messenger programs (Yahoo, AOL, MSN etc.) or social networking sites to communicate with students in or out of school.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet or in general.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.
- To safeguard employees only use your school email account to contact parents and students.

Social Networking

• All members of staff must be aware that, due to the ease of publishing information and content online, it is now very easy for staff to confuse writing in their capacity as a member of staff with sharing their own individual opinion.

- Staff must be aware that even as an individual, his/her actions could be criticized and seen as bringing a school into disrepute, especially if other users are aware of their role. This may have disciplinary, civil or even criminal consequences. It is crucial that all members of staff are made aware of the boundaries and professional practices online in order to protect their professional status.
- Staff should always remember that once content is shared online it is possible for it be circulated far wider than intended without consent or knowledge.
- It is therefore inappropriate for any member of staff, past or present to make any comments regarding any aspect of the school, its students or parents on any social or other networking site.

Please read this document carefully. If you violate these provisions action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____ Signature:_____

Date:_____

Please sign both copies. Keep one copy for your records and return the other to the finance office.

ST. JOSEPH'S COLLEGE
STUDENT USE OF ICT AGREEMENT

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe whilst using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk. The school will try to ensure that *students* will have good access to ICT to enhance their learning and will, in return, expect the *students* to agree to be responsible users.

Acceptable Use Policy Agreement

- I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.
- I will not disclose or share personal information about myself or others when on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.
- I will not steal, disable or cause any damage to school equipment, or the equipment belonging to others.

I will act as I expect others to act toward me:

- I will respect other peoples' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission. **I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:**
- I will only use my personal hand held / external devices (mobile phones / USB devices etc.) in school if I have and I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- I understand that if I am caught vandalizing or intentionally causing damage to any of the school systems, the cost of the damage can be invoiced to my parents.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

- I have read and understand the above and agree to follow these guidelines when:
- I use the school ICT systems and equipment (both in and out of school)
- I use my own equipment in school (when allowed) e.g. mobile phones, iPad, tablets, cameras etc.
- I use my own equipment out of school in a way that is related to me being a member of this school e.g. communicating with other members of the school, accessing school email, VLE, website etc.

Student's name: ……. Signature: …….. Date: ……

Parent's name: …… Signature: …….. Date: ……

Why we Filter the Internet

Introduction

Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is one item in the E-Safety toolbox that is of particular importance. When talking about an Internet filter there are two important aspects:

Very broadly speaking

- **Filtering** - this is a pro-active measure to ensure (as much as possible) or prevent users from accessing illegal or inappropriate (by age) websites.
- **Monitoring** - this is a reactive measure and for the most part means searching, browsing or interrogating filter logs (known as the cache) for Internet misuse.

These terms are important; mention to anyone that you are monitoring their Internet use and the immediate vision is of somebody sat at a computer screen watching every move and click; that is simply not the case.

The fact that an Internet filter is in place to filter and monitor activity is of particular importance because you then have questions raised of morality such as, "It's my human right to privacy", "big brother is watching", and others.

I happen to agree with this viewpoint, but at the same time I have no issues whatsoever with any monitoring whether it be online or not - as long as it is a justifiable reason and the expectations of that monitoring are set beforehand.

Consider CCTV at your school; everybody knows it is there because you can see it and there are (or should be) signs telling people that they are being monitored; everybody knows why it is there whether they agree with it or not. It is justified for the protection and safety of children and staff whilst in school, and also the protection of the building and its contents.

But what about Internet filtering? How many of your parents know that the online activity of their child may be monitored? How many of your staff know? Importantly, do they know why? Whilst the answer should be "yes" to all, I know that isn't the case and normally with good reason; how do you know what you don't know?

As with many things we do in life it is all about managing expectations, commonly known as justifying ourselves. But it is that justification that gives us precedence for doing something that others may deem controversial.

Why do we Filter and Monitor?

Schools filter Internet activity for two reasons:

We filter to ensure

- (as much as possible) that children and young people (and to some extent adults) are not exposed to illegal or inappropriate websites. These sites are (or should be) restricted by category dependent on the age of the user. Exposure would include browsing to specifically look for such material, or as a consequence of a search that returns inappropriate results.
- (as much as possible) that the school has mitigated any risk to the children and young people, and thereby reduces any liability to the school by making reasonable endeavours to ensure the safety of those children and young people.

We monitor for assurance

- (as much as possible) that no inappropriate or illegal activity has taken place.
- To add to any evidential trail for disciplinary action if necessary.

A right to privacy?

Everybody has a right to privacy, whether adult or child. But in certain circumstances there is a reduced expectation of privacy. In the context of this guide, that reduction is for security and safeguarding. This expectation is applicable whether it is school-owned equipment, or personally owned equipment used on the school network (and in some cases even if that personally owned equipment isn't used on the school network, but is used in school or for school business).

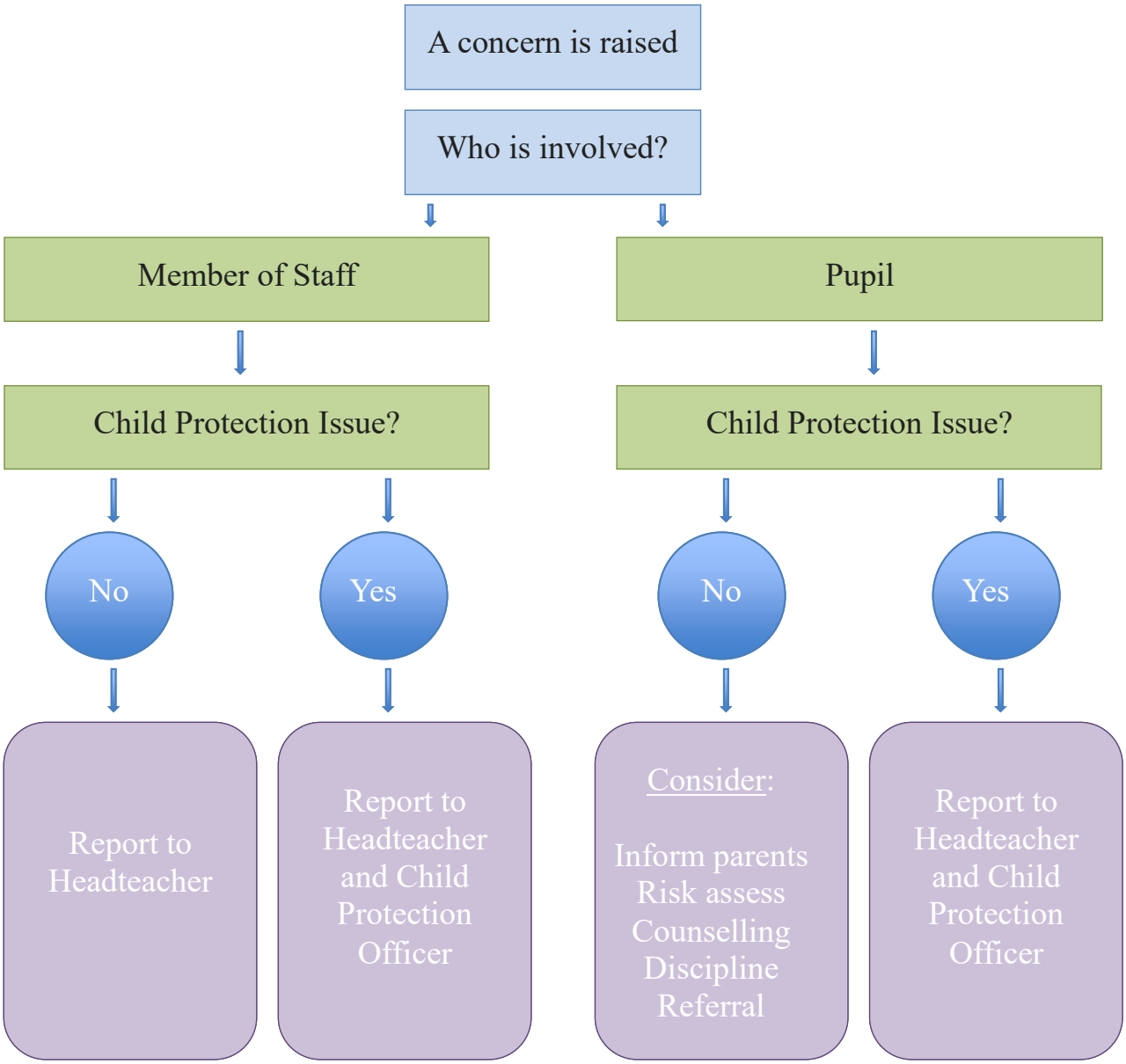
Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however you are required by law (Data Protection Act 1998) to make all reasonable efforts to inform users that you are monitoring them. By making reasonable efforts you are working "with" the students and parents, not just merely telling them.

In reality, very few schools actually monitor Internet activity, and neither do local authorities or RBC's (remember, monitor is different to filter). Whether that is right or not is out of scope for this paper, but the fact is you could; in fact Ofsted make clear that schools should be managing their own filter, and this would include monitoring for inappropriate activity, overly-restrictive filtering or otherwise.

Of course, some will disagree with what you are doing, but that is their right and again consent is not a requirement. It is the understanding, not the consent that is important.

Inappropriate Activity Flowchart



If you are in any doubt, consult the Headteacher, Child Protection Officer or Safeguarding