St Nicolas CE Primary School
E-SAFETY POLICY

CURRICULUM LEAD SIGNATURE:
(Phil Gaskin)

DATE ADOPTED: Mar 2021

DATE FOR REVIEW: Mar 2023

Additional notes:

Cross reference with the following policy/ies:
Anti-bullying policy
Safeguarding policy
Computing policy

St Nicolas CE Primary School
E- Safety Policy

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, guardian, 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, agents and / or visitors.

Safeguarding is a serious matter; at St Nicolas CE Primary School 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 Nicolas CE Primary School 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 Students Acceptable Use Policy will be sent home to parents electronically at the beginning of each school year. Parents will give their acceptance of the terms and conditions and 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 e-Safety 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.
- The designated E-Safety Officer has had appropriate CPD in order to undertake the day-to-day duties.
- All E-safety incidents are dealt with promptly and appropriately.

E-Safety Officer
The day-to-day duty of the E-Safety Officer is devolved to the Computing Coordinator (Phil Gaskin)

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.
- Ensure any technical e-safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Make him/herself aware of any reporting function with technical e-safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

ICT Technical Support Staff

TurnITOn ICT 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.
    - The IT System Administrator password is to be changed on a termly basis.

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 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.
- The reporting flowcharts contained within this e-safety policy are fully understood.

All Students

The boundaries of use of computing equipment and services in this school are given in the student Acceptable Use Policy; any deviation or misuse of computing equipment or services will be dealt with in accordance with the behaviour policy. An 'Internet Permission' form is completed on entry to the school.

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 parents evenings, school newsletters and e-safety workshops 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 computing equipment or services.

Curriculum Link Governor

During the academic year, the E-safety officer (computing coordinator) regularly meets with the curriculum link governor. They are responsible for:

- advising on changes to the E-safety policy.
- establishing the effectiveness (or not) of E-safety training and awareness in the school.
- recommending further initiatives for E-safety training and awareness at the school.

Technology

St Nicolas School uses a range of devices including PC's, laptops and tablets. 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 Surfprotect 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 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 Microsoft Exchange On-line Protection software (for Microsoft office365) that prevents any infected email to be sent from, 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.

Encryption – Data transfers for school-to-school information uses appropriate encrypted software. Any breach (i.e. loss/theft of device such as laptop) is to be brought to the attention of the Headteacher immediately. Staff records are managed in SIM's. Full access to these records is limited to the Business Manager and Administrator only. Pupil records are managed in Sim's and limited access is granted to all staff except the admin team and Business Manager. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office.
(Note: Encryption does not mean password protected.)

Passwords – all staff and students will be unable to access any device without a unique username and password. Staff and student passwords will change on a regular basis or if there has been a compromise, whichever is sooner. The Computing Coordinator and IT Support will be responsible for ensuring that passwords are changed. The IPAD's are not password protected however; they are limited to what the class teachers allows.

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.

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 (Appendix 1); students upon signing and returning their acceptance of the Pupils Acceptable Use Policy, or parental signing if required (Appendix 2).

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.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photographic Policy, and is re-iterated here for clarity. 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.

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.
- There is to be no identification of students using first name and surname; first name only is to be used.
- Where services are "comment enabled", comments are to be set to "moderated".
- 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 school's 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 (Appendix 3).

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 Nicolas School will have an annual programme of training which is suitable to the audience.

E-Safety for students is embedded into the curriculum; whenever computing 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. There is a broad and cross-curricular 'digital literacy' curriculum taught at St Nicolas. This links to the PSHCE/SEAL's values that are taught across the school. The curriculum covers how to stay safe online and how to be a responsible digital citizen. This information is highlighted each year on 'Safer internet Day' and underpins the activities and tasks the children complete.

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.

The E-Safety Training Programme can be found within the Computing Coordinators file.

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; 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.

Explaining to parents, staff and students
As previously mentioned, it is the understanding that is important, not the consent. It is not appropriate to simply have a sentence in the school e-Safety or Acceptable Use Policy and for that to suffice; privacy is always an emotive issue.

Here are the "must do's":

- Statement in E-Safety Policy, e.g. "All staff, students and parents of students will be informed that Internet activity may be monitored in order to ensure as much as possible that users are not exposed to illegal or inappropriate websites, and to ensure as much as possible that users do not actively seek access to illegal or inappropriate websites," or words to that effect. You would then briefly explain why.
- Statement in Acceptable Use Policy, e.g. "Users are reminded that Internet activity may be monitored". That's it, you don't need anything more than that. Don't forget, the AUP is simply a concise "cut-out-and-keep" version of the e-Safety Policy containing the rules.
- Explain to staff why monitoring is important, allow them to voice any concerns and set their expectations of how the data can be used.
- Explain to the students as well, allow them to ask questions.
- A letter home to parents, again explaining that the Internet activity may be monitored, and why. Assure the parents that you talk to the students, who are allowed to voice concerns and ask questions. This letter would normally form a part of the term 1 paperwork; ideally it would include the Acceptable Use Policy and a signature sheet. Parents (and students if old enough) should sign the letter to say they understand, not to agree as again, consent is not required.
- Don't forget, Ofsted require that schools engage with parents and students when creating policy.

Summary

- Filtering is different to monitoring.
- You do not require consent.
- But you must tell users if you do monitor, or if you have the facility to monitor.
- Set user expectations; explain under what circumstances it may be a requirement to monitor.
- Ensure you have a good statement in your E-Safety Policy.
- Ensure you have informed users that Internet use “May be subject to monitoring” in your Acceptable Use Policy.
- Ensure parents are informed, the reason why monitoring may take place, and they sign as read and understood.

Appendix 1

ICT Acceptable Use Policy (AUP)
Pupils

Safety and Responsibilities Policy – Pupil / Student

- This policy relates to the use of any type of computer (including, but not limited to: desktop PCs, laptops, tablet devices, smart phones and other smart devices [such as smart watches or other wearables])
- All pupils must follow the rules detailed below when using computers in the school and any web-based services which the school uses. This list cannot cover every eventuality and it will be regularly updated. Children are expected to behave at all times in a way that adheres to the school ethos
- If pupils do not follow the rules they may find that they are no longer allowed to use the computers or that they have restricted access to the computers and school web services. Furthermore, pupils who misuse the computers may have their past network usage investigated and, in some circumstances, information may be passed on to the appropriate authorities

Computer Rules

1. Equipment, logging in and using the school network.

- I will treat computer equipment carefully and with respect; cables will not be unplugged without permission from a member of staff, computers will be shut down properly and mobile devices will be handled carefully by one child at a time
- I will only use my own log in details when using a computer and I will make sure that I log out when I have finished. If I think someone knows my log in details I will let a member of staff know
- I will never use log in details belonging to another child and if a computer I am about to use is already logged in, I will log out the user before I begin to work. I will log off any unattended computers at the end of a lesson
- I will not share my own computer log in details (username and password) with anyone else.
- I will not share my log in details for any web services with anyone else
- I understand that the staff at the school are able to view my work at any time (during a lesson or saved work on the network)
- I will keep my personal details private when using the internet (I will not share my name or details about myself)
- I will save my work in the folders I am instructed to by my teachers
- I will never attempt to open the work of other children, nor will I change or delete the work of another child
- I will never try to use the school network in a way which could cause problems for other users

2. Network security

- I will never try to download and install software onto the school computers
- I will never bring removable media such as USB memory sticks into school and connect them to a school computer without the permission of a teacher (who will check it for viruses and malware before it is used)
- I will not open emails from unknown senders or suspicious links in emails
- I will not attempt to visit websites which are not appropriate to children of primary school age
- I will not click on advertising or any other links on websites unless approved by my teacher

3. E-Safety and personal responsibility

- I will not try to access social media sites or chat rooms (unless they are part of a school approved and monitored virtual learning environment – such as Purple Mash or Frog)
- I understand that emails sent using a school system may be viewed and monitored by school staff
- I will not attempt to contact school staff through digital media (such as social networks, email and text messaging), unless it is on one of the school's own networks set up for this purpose
- I will not try to upload photos of myself or others to the internet
- I will not share personal information about myself or others on the internet
- I will think carefully about what I post on the internet, as I may unintentionally hurt the feelings or other people or cause distress
- I understand that a lot of the content on the internet is subject to copyright and I am not allowed to publish copyrighted materials without permission
- I understand that I am below the age normally recommended for the use of social media apps (such as, but not limited to: Facebook, Instagram, WhatsApp, Viber, Facetime, Skype, Snapchat…) and that if I am using these services my parents should be aware of this fact (KS1-KS3)
- I understand that if I post things about others on social media outside school there may be repercussions in some circumstances (such as the school, or in some cases, other outside agencies becoming involved)
- I understand that if others have been posting information about me online without my consent or information which makes me uncomfortable I should report it to my parents / carers and an adult at the school (where the people at the school are involved)
- I understand that if I have worries or concerns about what I have seen on the internet or activities in which other pupils are engaged, I can always report this to a member of the school staff and the school will do its best to support and help me
- I will not use inappropriate language (such as swear words or words which are likely to cause offence to others, based on their appearance, lifestyle, religion or ethnic background)
- I will not try to visit websites or access information which contains illegal or inappropriate material (such as websites which may encourage hatred or extreme views against other people based on their looks, religion, lifestyle or origins). I understand that if I do attempt to access these materials the police and / or other local authorities may be contacted to investigate me
- I understand that I have a personal responsibility to behave responsibly and respectfully on the school network and the internet

ICT Acceptable Use Policy (AUP)
Safety and Responsibilities Policy – Pupil / Student

Pupil User Agreement Form

- I agree to follow the rules and the spirit of the rules when using school computers, tablet devices, the school network, school websites and services
- I agree to report any misuse of school computers, tablet devices or the school network to school staff
- I agree to report any inappropriate websites accessed on the school network to school staff
- I understand that if I break the rules I may have my access to computers restricted and I may be investigated by the school and outside agencies

Pupil printed name (capital letters): …….

Pupil Signature: ……

Date: ……..

Parent / Guardian printed name (capital letters): ……..

Parent / Guardian Signature: ……

Date: …….

Appendix 3

E-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	
Signature (Governor)		**Date:**	

Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content - staff	1	3	3	e-Safety Officer IT Support
1.	Internet browsing	Access to inappropriate/illegal content - students	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: **The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.**
Final decision rests with Headteacher and Governing Bod

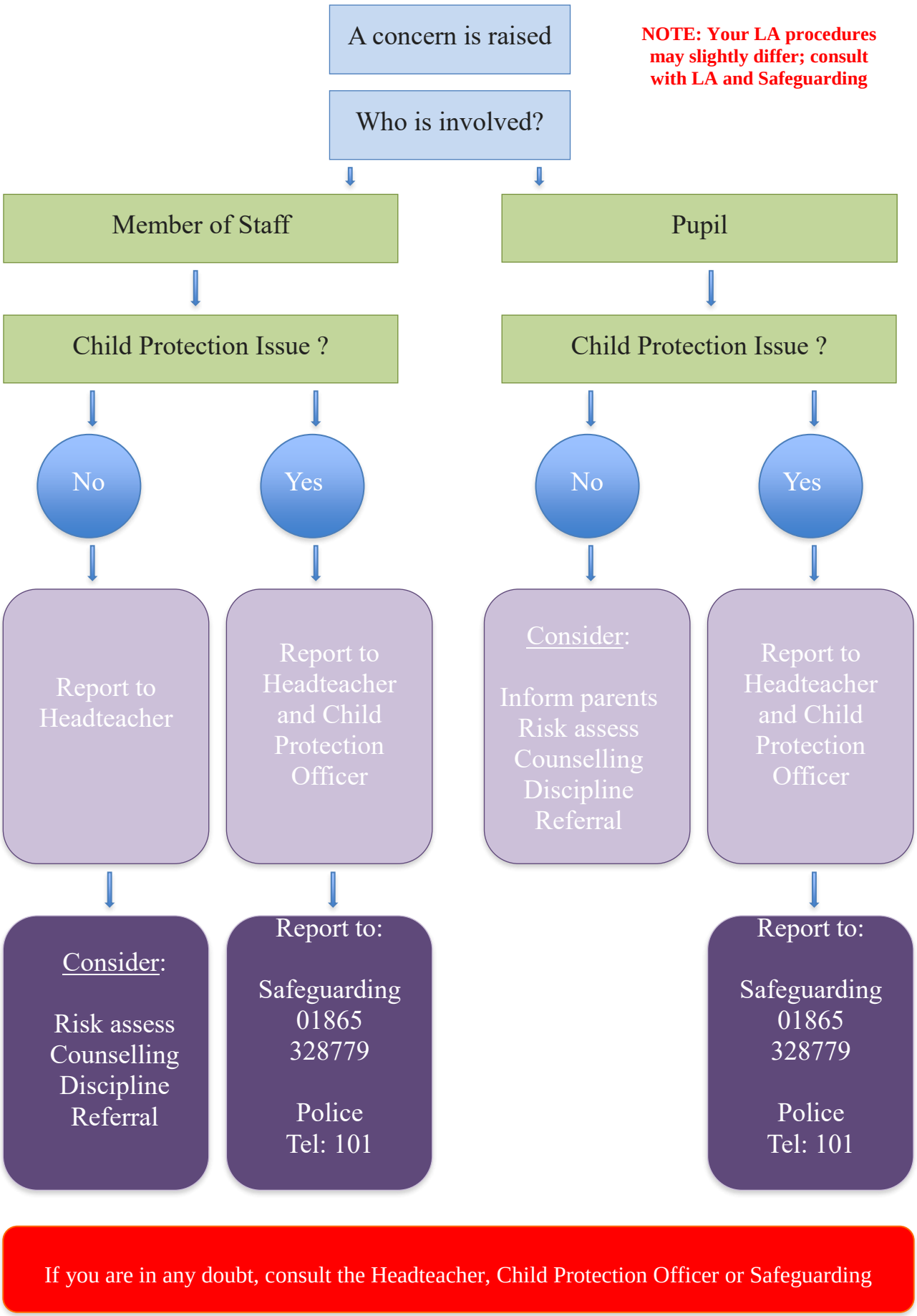
Risk Assessment

Risk No.	Risk
3	In certain circumstances, students will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; students will potentially have unrestrComputinged access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the student to undertake this work at home, the school has a common law duty of care to ensure, as much as is reasonably possible, the safe and well being of the child.
LIkelihood 3	The inquisitive nature of children and young people is that they may actively seek out unsavoury online content, or come across such content accidentally. Therefore the likelihood is assessed as 3.
Impact 3	The impact to the school reputation would be high. Furthermore the school may be held vicariously liable if a student accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the student.
Risk Assessment	HIGH (9)
Risk Owner/s	e-Safety Officer IT Support
Mitigation	This risk should be actioned from both a technical and educational aspect: Technical: Laptop is to be locked down using XXXXXXXX software. This will mean that any Internet activity will be directed through the school Internet filter (using the home connection) rather than straight out to the Internet. The outcome is that the student will receive the same level of Internet filtering at home as he/she gets whilst in school. Education: The e-Safety Policy and Acceptable Use Policy will be updated to reflect the technical mitigation. Both the student and the parent will be spoken to directly about the appropriate use of the Internet. Parents will be made aware that the laptop is for the use of his/her child only, and for school work only. The current school e-safety education programme has already covered the safe and appropriate use of technology, students are up to date and aware of the risks.

Approved / Not Approved (circle as appropriate) **Date:**

Signed (Headteacher) : **Signed (Governor) :**

Inappropriate Activity Flowchart



Illegal Activity Flowchart