St Nicolas CE Primary School
E-SAFETY POLICY

CURRICULUM LEAD SIGNATURE: 

(Camilla Crask)

DATE ADOPTED: January 2024

DATE FOR REVIEW: January 2025

Additional notes:

Cross reference with the following policies:

Anti-bullying policy
Safeguarding policy
PSHE policy

St Nicolas CE Primary School
E- Safety Policy

Policy Statement
The E-safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, students and any other person.

Parents – any adult with a legal responsibility for the child/young person e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site including visits, conferences and school trips.

Wider school community – students, all staff, governing body, parents, agents and/or visitors.

This policy covers the key principles of e-safety. At St Nicolas CE Primary School, we use technology and the internet across all areas of the curriculum. Computing and the use of digital devices is an essential resource to support learning and teaching and plays an important role in the everyday lives of children, young people and adults. Online safeguarding, known as e-safety 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. It is an integral part of safeguarding and requires a whole school, cross-curricular approach and collaboration between key school leads. Accordingly, this policy is written in line with 'Keeping Children Safe in Education' 2023 (KCSIE), 'Teaching Online Safety in Schools' 2019, statutory RSHE guidance 2019 and our school PSHE policy. Any issues and concerns with online safety must also follow the school's safeguarding and child protection policies and procedures.

The primary purpose of this policy is to:

- Establish the guidance that we have in school for using the internet in order to minimise foreseeable harm to a student or liability to the school.
- Ensure the whole school community uses the internet safely, effectively and responsibly.
- Raise the awareness of staff and students to the benefits of internet access whilst ensuring that the use of digital technology is in line with the standards and expectations of the school.
- Protect the school from undesirable content and ensure risks are quickly identified, assessed and mitigated (where possible).
- Support students when learning at home.

This policy is available on the St Nicolas CE Primary School website. Upon review, all members of staff will sign and adhere to both the e-safety policy and the Staff Acceptable Use Policy. A copy of this policy and the Student Acceptable Use Policy will be sent home to parents and carers electronically (or in paper form where the school does not have an email address). Parents/carers must give their acceptance of the terms and conditions in order that students can 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 annually and in response to significant e-safety incidents so that it is up to date, covers all aspects of technology use within the school and ensures e-safety incidents have been appropriately dealt with. They will also ensure that incidents are managed effectively.
- Appoint one governor to have overall responsibility for the governance of e-safety at the school.
- Ensure that children are taught about how to keep themselves and others safe online. This will be tailored to the specific needs and vulnerabilities of individual children, including children who are victims of abuse, and children with special educational needs and/or disabilities.

Curriculum Link Governor

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

- Monitoring changes to the E-safety policy and its effectiveness in the school.
- 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.
- Keep up to date with emerging risks and threats through technology use.
- Receive updates from the Headteacher where required regarding significant risks/incidents.

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:

- The designated safeguarding lead takes lead responsibility for safeguarding and child protection including online safety and understanding the filtering and monitoring systems and processes in place.

- All staff receive online safety training which includes an understanding of the expectations and applicable roles and responsibilities in relation to filtering and monitoring. In addition, all staff should receive online safety updates as required, and at least annually, to continue to provide them with relevant skills and knowledge to safeguard children effectively.

- All staff are aware of indicators of abuse and neglect, understanding that children can be at risk of harm online.
- 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 and other relevant staff receive suitable CPD to enable them to carry out their online safety role.
- All E-safety incidents are dealt with promptly and appropriately.
- They and at least another member of senior leadership team are aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff.

E-Safety Officer

The day-to-day duty of the E-Safety Officer is devolved to the Computing Coordinator, Camilla Crask. 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 and 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.
- Record e-safety incidents ensuring staff know what to report along with appropriate audit trail.
- Ensure technical e-safety measures in school (e.g. internet filtering software) are fit for purpose through liaison with the local authority and/or ICT Technical Support.
- Be 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.
- 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 and not open to misuse or malicious attack. 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.
- The school meets required online safety technical requirements and any local authority/other relevant body online safety policy or guidance that may apply.
- Filtering levels are applied appropriately according to the age of the user and that categories of use are discussed and agreed with the e-safety officer and Headteacher.
- Users may only access networks and devices through a properly enforced password protection policy. The same password should not be used on multiple sites.
- The IT System Administrator password is to be changed on a termly basis.
- Any suspected misuse or problem is reported to the online safety coordinator.

All Staff

Staff are to ensure that:

- They are aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse and other risks online. In many cases abuse and other risks will take place concurrently both online and offline. Children can also abuse other children online, this can take the form of abusive, harassing, and misogynistic/misandrist messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography to those who do not want to receive such content.

- They understand that children can abuse other children (often referred to as child-on-child abuse), and that it can happen online. All staff should be clear as to the school's safeguarding policy and procedures with regard to child-on-child abuse and the important role they have to play in preventing it and responding where they believe a child may be at risk from it.

- They have current internet safety knowledge as well as awareness of the current school online safety policy and practices. Anything not understood should be brought to the attention of the Headteacher.

- Any E-safety incident must be reported to the E-Safety Officer 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.

- Online safety issues are embedded in all aspects of the curriculum.

- Students understand and follow the online safety policy.

- Use of digital technologies such as iPads, mobile devices and cameras are monitored in lessons.

- Children are guided to sites that have been checked and are suitable for use in pre-planned computing lessons. Where this is not possible, sites to be closely monitored.
- All digital communications with pupils and parents/carers must be on a professional level and only carried out using official school systems.

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 according to the behaviour policy. An 'Internet Permission' form is completed on entry to the school.

E-Safety is embedded into our curriculum so that students understand the importance of adopting good online safety practice when using digital technologies. Students will be given advice and guidance by staff in order that they understand the importance of reporting abuse, misuse or access to inappropriate materials whilst at school or outside of school.

Parents/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.

Remote education

Communications with parents/carers should be used to reinforce the importance of children being safe online and to ensure they understand what systems are in place in school to filter and monitor online use. It is especially important for parents/carers to be aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school their child will be interacting with online for example on Teams.

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 Securly to prevent 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 online 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 SIMs. Full access to these records is limited to the Business Manager and Administrator only. Pupil records are managed in SIMs 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 IPads are not password protected but they are limited to what the class teachers allows.

Anti-Virus – All capable devices 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. Users are reminded that internet activity may be monitored.

Photos and videos – Digital media such as photos and videos are covered in the schools' Digital Imagery & Photography Policy and is reiterated here for clarity. All parents must sign a photo/video release slip; 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 Digital Imagery & Photography 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.

The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four areas of risk:

Content
Being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

Contact
Being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

Conduct
Online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.

Commerce
Risks such as online gambling, inappropriate advertising, phishing and or financial scams.

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.

We will establish further training or lessons as necessary in response to any incidents.

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.

Online Safety Contacts and References

- CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk
- Childline: www.childline.org.uk
- Childnet: www.childnet.com
- UK Council for Internet Safety:
- www.gov.uk/government/organisations/uk-council-for-internet-safety
- Cybermentors: www.cybermentors.org.uk
- NSPCC Online Safety: www.learning.nspcc.org.uk/online-safety
- Internet Watch Foundation (IWF): www.iwf.org.uk
- The National College: www.nationalcollege.com/categories/primary-online-safety
- Think U Know website: www.thinkuknow.co.uk
- Virtual Global Taskforce: www.nationalcrimeagency.gov.uk/virtual-global-taskforce
- Report Child Abuse: https://www.gov.uk/report-child-abuse-to-local-council

Appendix 1

ICT Acceptable Use Policy (AUP)
Pupils

Safety and Responsibilities Policy – Pupil

- 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

- The school's online safety Policy covers my actions out of school, if related to my membership of the school.
- I will not attempt 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 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, Tik Tok, 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 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.

Appendix 2

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

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.
- I understand the importance of adopting good online safety practice when using digital technologies.

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**

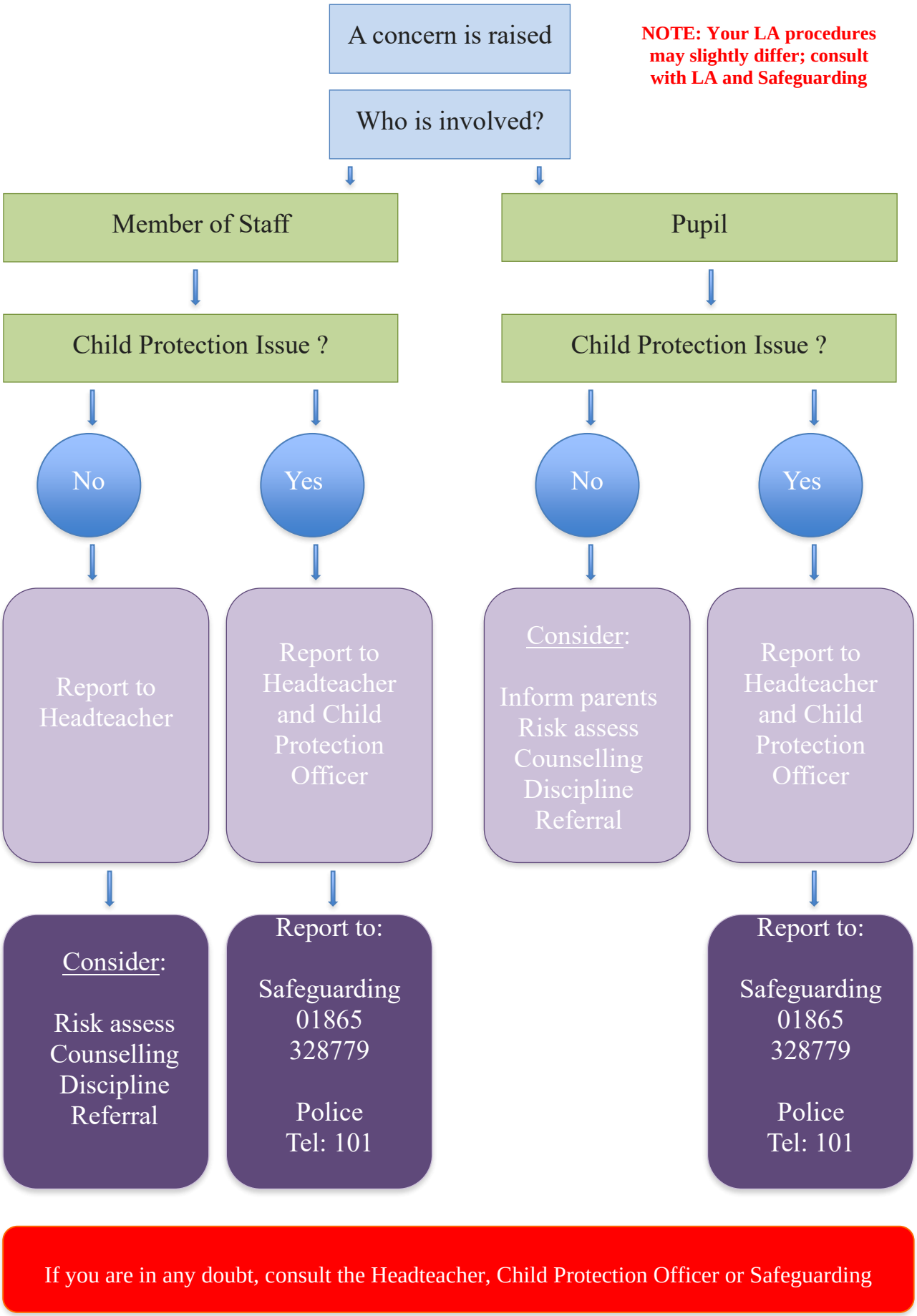
Risk Assessment

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 Securly 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