eSAFETY Policy

Edenham CE Primary School

School's Policy Date: July 2017
School's Policy Review Date: September 2017
Next Review date; Annual – September 2018

Chair to the GB; Mrs Sukey Brewster
ESafety Governor; Mr Tom McWilliams
School's eSafety officer; Mrs Kris Radford-Rea
School's IT support provided by; Ark ICT

Table of Contents

Introduction

The e-Safety Policy is important in school for a number of reasons, including:

- To ensure there is a clear and consistent approach responding to incidents.
- To ensure that every person responsible for the children is fully aware of his/her responsibilities.
- To set boundaries of use (goalposts) of any school owned IT equipment, or personal IT equipment used in the school, and set the boundaries of services such as social networking (e.g. blogging, Twitter).

Policy Statement

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

Users - refers to staff, Local Governing Board, school volunteers, pupils 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 – pupils, staff, Academy Trust employees, contractors, Local Governing Board and parents.

Safeguarding is a serious matter. At Edenham Primary School we use technology and the Internet across many 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 pupil or liability to the school.

This policy is available for anyone to read on the Edenham Primary School website.

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 Pupils Acceptable Use Policy will be sent home with pupils 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, pupils will be permitted access to school technology including the Internet.

Policy Governance (Roles & Responsibilities)

Local Governing Board

The Local Governing Board is accountable for ensuring that our school has effective policies and procedures in place. As such it will:

- Review this policy 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, that e-safety incidents are appropriately dealt with and that the policy was effective in managing such 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 Head Teacher in regards to training, identified risks and any incidents.
    - Lead on e-Safety matters during Management and other governing Board meetings.

Head Teacher

Reporting to the Local Governing Board, the Head Teacher has overall responsibility for e-safety within our school. It is the intention of this policy that the Head Teacher acts as the school e-Safety Officer. In the event of Head Teacher absence or other work commitments, the day-to-day management of this policy is delegated to Mrs Sian Hawes, who will act as the designated deputy e-Safety Officer. Throughout the rest of this policy where mention is made of the Head Teacher's responsibilities, it is to be assumed that in the absence of the Head Teacher the same responsibilities rest with the deputy e-Safety Officer.

The Head Teacher will ensure that:

- E-Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. senior leadership team, all staff, designated e-Safety Officer, deputy e-Safety Officer, pupils, Local Governing Board and parents.
- All e-safety incidents are dealt with promptly and appropriately.

e-Safety Officer

The e-Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology; familiarise 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 e-Safety governor.
- Advise the e-Safety governor on all e-Safety matters.
- Engage with parents and the school community on e-Safety matters at school and at home.
- 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 ICT Technical Support.

- Make herself aware of any reporting function with technical e-Safety measures, i.e. internet filtering reporting function; liaise with the e-Safety governor to decide on what reports may be appropriate for viewing.

ICT Technical Support

ARK ICT Solutions (Pinchbeck, Spalding) has the school contract to manage our ICT systems and provide technical support. For the purposes of this policy, ARK ICT Solutions is treated as a member of the school staff and will agree to ensure that their employees adhere to the spirit of this policy when dealing with Edenham Primary School matters.

The 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.
    - Operating system updates are regularly monitored and devices updated.
    - Any e-Safety technical solutions such as Internet filtering are operating correctly.
    - In agreement with the Head Teacher, filtering levels are applied appropriately and according to the age of the user.
    - Passwords are applied correctly to all users regardless of The IT System
    - Administrator password is changed on a calendar monthly basis.
    - Individual user passwords are changed at the beginning of each school term.

Staff

Staff members 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 Head Teacher.
- Any e-safety incident is reported to the Head Teacher immediately and that a written e-Safety incident report is raised before the start of the following school day.
- The reporting flowcharts contained within this e-safety policy are fully understood.

Note: If a member of staff is unsure of the need to raise a report, he/she is to discuss the matter with the Head Teacher.

Pupils

The boundaries of use of ICT equipment and services in this school are given in the Pupil Acceptable Use Policy; 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; pupils will be given the appropriate advice and guidance by staff. Similarly, it will be explained to all pupils how to 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 assist parents in developing the skills and knowledge they need to ensure the safety of children outside the school environment. The Head Teacher will keep parents up to date with new and

emerging e-Safety risks, and will involve parents in strategies to ensure that pupils are empowered to deal with these risks.

Parents must accept that the school needs have to rules in place to ensure that our children are properly safeguarded. As such, parents are required to sign the Pupil Acceptable Use Policy before they or their children are granted access to school ICT equipment or services.

e-Safety Governor

The designated e-Safety governor is Tom McWilliams. As the lead governor responsible for e-Safety matters, he will:

- advise the Local Governing Board on changes to the e-Safety policy.
- analyse the effectiveness of e-Safety training and awareness in the school.
- recommend further initiatives for e-Safety training and awareness at the school.

Technology

Edenham Primary School uses a range of electronic devices. In order to safeguard the pupil, and in order to prevent loss of personal data, we employ the following assistive technology:

Internet Filtering – we use 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, Head Teacher and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Head Teacher and e-Safety governor as soon as practical.

Email Filtering – we use software that prevents any infected email to be sent from the school, or to be received by the school

Passwords – Access to any device requires a unique user username and password. Staff passwords are changed on a termly basis or if there has been a compromise, whichever is sooner. Staff must NOT share their passwords with anyone else including colleagues, volunteers etc.

Pupil passwords are provided to pupils by the school as required. The Head Teacher has full access to all pupil accounts.

Where it is not possible to password protect or encrypt a device, a risk assessment is to be made and a record of the case made to use such devices is to be raised and attached to this policy by the Head Teacher.

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 Head Teacher if there are any concerns. All mobile devices are automatically assessed by the virus protection software when they are connected to a computer. Complete scans of these peripheral devices can be run via the software dashboard.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted upon receipt of a correctly signed e-Safety Acceptable Use Policy form. Parents are required to sign and return these forms on behalf of their children. Access to the Internet is monitored and such access may be withdrawn in the event of any breach of the e-Safety Acceptable Use Policy.

Email – All staff are reminded that emails are subject to Freedom of Information requests. As such, emails of a personal nature are not permitted and the service is to be used for professional work-based emails only. Similarly, the use of personal email addresses for work purposes is not permitted.

Pupils do have access to the school email system and will be taught how to send and receive emails during lesson time.

Photos and videos – Digital media such as photos and videos are covered in the school's 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.

Social Networking – there are many social networking services available; Edenham Primary School 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. The following social media services are permitted for use within the school and have been appropriately risk assessed. Should staff wish to use other social media, the Head Teacher's permission must first be sought. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and pupils in school.
- Twitter – used by the school as a broadcast service.
- Facebook – used by the school as a broadcast service.

Note: A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.
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 pupils 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 Head Teacher. The Head Teacher will assist in taking the appropriate action to deal with the incident. An e-Safety incident report is to be completed and filed in the e-Safety Incident Log before the start of the following school day (where this would lead to a delay of more than 48 hours, the report is to be completed and filed before the end of that school day).

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, our school has an annual programme of training tailored to meet the needs of the applicable audience.

e-Safety for pupils 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 pupil's learning.

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

In consultation with the e-Safety governor, the Head Teacher will recommend a programme of training and awareness for the school year. Should any member of staff feel they have had inadequate or insufficient e-Safety training this must be brought to the attention of the Head Teacher who will authorise further training as necessary.

Appendix 1 Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet and return it to the Head Teacher.

Internet access - You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an e-Safety incident, reported to the Head Teacher and an e-Safety incident report completed.

Social networking – is allowed in school in accordance with the e-Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children. As a general rule, Staff should not become "friends" with parents or pupils on personal social networks. However, as we are a small and close-knit community, some Staff members may already be "friends" with parents on social media. Staff members are to refer to the Staff Code of Conduct to ensure that they do not inadvertently compromise the spirit of this policy.

Use of Email – staff are not permitted to use school email addresses for personal business. All email should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act. Likewise, personal email addresses should not be used for school business for the same reason.

Passwords - Staff should keep passwords private. There is no occasion when a password needs to be shared with another member of staff or pupil, and only rarely with IT support (afterwhich, it should be reset by the staff member).

Computer Configuration - All computers are on the school domain. As such, any user can log-on hen on-site and connected to the domain. Staff laptops each have their personal folder. This folder can be synchronised for use when off-line and not connected to the domain.

Data Protection – If it is necessary for you to take work off site, you should ensure that your device is stored securely and properly logged-off when not in use. On no occasion is data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head Teacher who will set the boundaries of personal use.

Images and Videos - You should not upload onto any internet site or service images or videos of yourself, other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings).

Use of Personal ICT - use of personal ICT equipment is at the discretion of the Head Teacher. Permission must be sought stating the reason for using personal equipment; a case is to be made by the individual and a risk assessment will be carried out by the Head Teacher.

Viruses and other malware - any virus outbreaks are to be reported to the ARK Solutions Limited helpdesk as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school (Telephone 0845 459 4900).

e-Safety – like health and safety, e-Safety is the responsibility of everyone to everyone. As such you will promote positive e-Safety messages in all use of ICT whether you are with other members of staff or with pupils.

Name:

Signature: **Date:**

Appendix 2 Letter to Parents/Carers

– eSafety and Pupil Acceptable Use Agreement

Dear Parent/Carers

Use of the Internet in school is a vital part of the education of your son/daughter. Our school makes use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

You will be aware that the Internet is host to a great many illegal and inappropriate websites and, as such, we will ensure as far as possible that your child is unable to access such sites. We are able to do this using advanced software known as an Internet filter. This filter categorizes websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child.

The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school. In order to ensure that there have been no attempts of inappropriate Internet activity, we may occasionally monitor these logs. If we believe there has been questionable activity involving your child we will inform you of the circumstances.

At the beginning of each school year we explain the importance of Internet filtering to your child. Furthermore, we explain that there has to be a balance of privacy and safety. We also inform our pupils that we will monitor their activity. All children are given the opportunity to ask questions and give their viewpoint. We would like to extend that opportunity to you also; if you have any questions or concerns please contact the Head Teacher Kris.Radford@edenham.lincs.sch.uk.

Yours Sincerely

Kris Radford-Rea

Before signing this letter, please take your child through the attached Charter of Good Online Behaviour, obtain their signature and return the signed charter with this letter.

I have read this letter and understand that my child's Internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the school network. I acknowledge that this has been explained to my child and that he/she has had the opportunity to voice their opinion, and to ask questions.

Name of Parent/Guardian:

Name of Child:

Signature: Date:

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

I Promise – to only use the school ICT for schoolwork that the teacher has asked me to do.

I Promise – not to look for or show other people things that may be upsetting.

I Promise – to show respect for the work that other people have done.

I will not – use other people's work or pictures without permission to do so.

I will not – damage the ICT equipment and if I accidentally damage something I will tell my teacher.

I will not – share my password with anyone. If I forget my password I will let my teacher know.

I will not – use other people's usernames or passwords.

I will not – share personal information online with anyone.

I will not – download anything from the Internet unless my teacher has asked me to.

I will – let my teacher know if anyone asks me for personal information.

I will – let my teacher know if anyone says or does anything to me that is hurtful or upsets me.

I will – be respectful to everyone online; I will treat everyone the way that I want to be treated.

I understand – that some people on the Internet are not who they say they are, and some people can be nasty. I will tell my teacher if I am ever concerned in school, or my parents if I am at home.

I understand – if I break the rules in this charter my parents will be told and my permission to use to the school systems may be withdrawn from me.

Signed (Pupil):

Date:

Appendix 3

Why we Filter the Internet?

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?

Everyone 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, pupils and parents/guardians of the pupils. 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 pupils 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.

Explaining to parents, staff and pupils

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, pupils and parents of pupils 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 Acceptable Use Policy 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 pupils 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 pupils, 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 pupils 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 the wider school community when creating policy as far as possible.

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 4 e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(Head Teacher or deputy 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 (Head Teacher)		**Date:**	
Signature (e-Safety Governor)		**Date:**	

Appendix 5 Risk Log (example)

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 - pupils	2	3	6	
2.	Blogging	Inappropriate comments	2	1	2	
2.	Blogging	Using copyright material	2	2	4	
3.	Pupil laptops	Pupils 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 Head Teacher and Governing Board.**
Final decision rests with Head Teacher and Governing Bod

Risk Assessment (example)

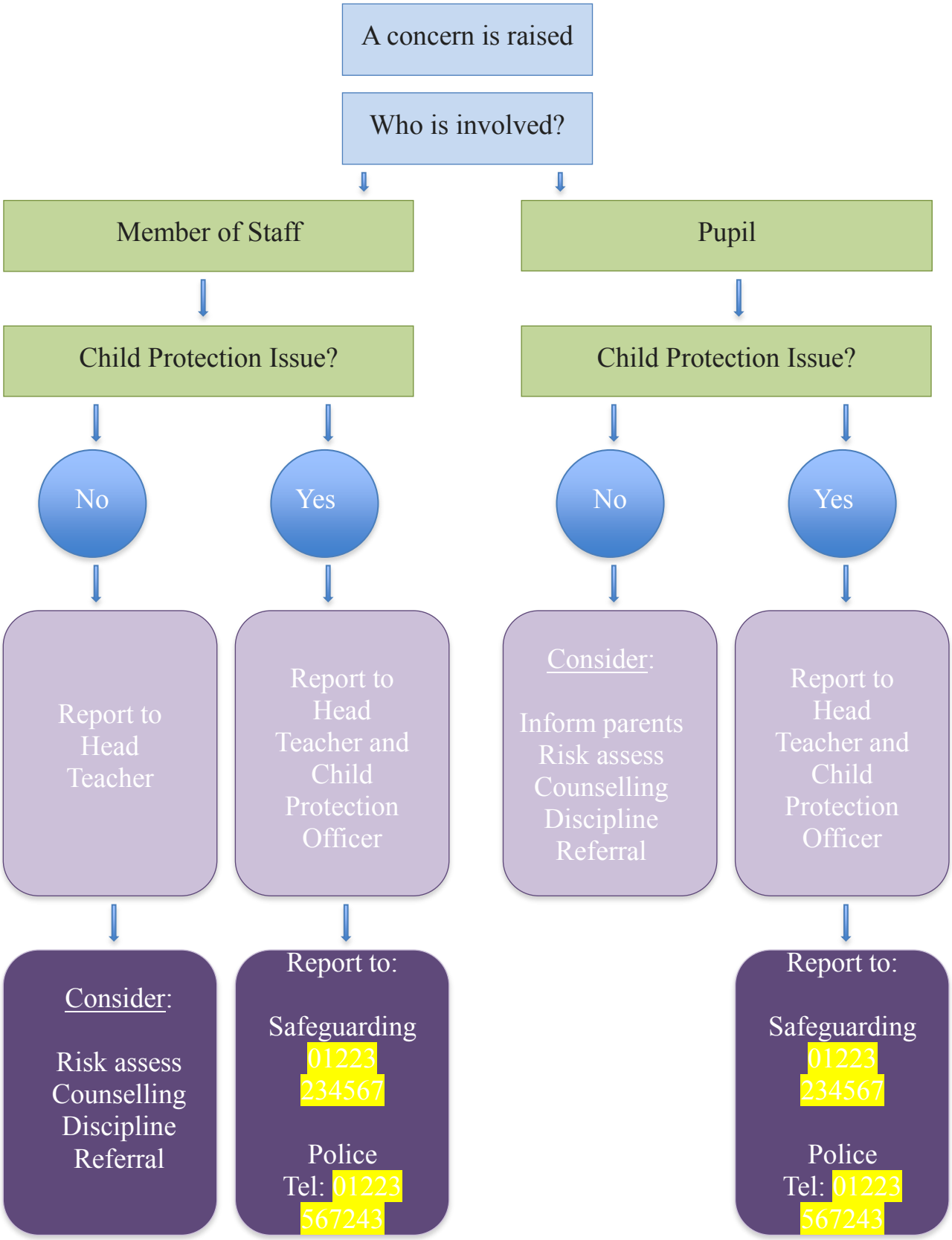
Risk No.	Risk
3	In certain circumstances, pupils will be able to borrow school-owned laptops to study at home. Parents may not have internet filtering applied through ISP. Even if they do there is no way of checking the effectiveness of this filtering; pupils will potentially have unrestricted access to inappropriate/illegal websites/services. As the laptops are owned by the school, and the school requires the pupil 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 pupil accesses illegal material using school-owned equipment. From a safeguarding perspective, there is a potentially damaging aspect to the pupil.
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 pupil 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 pupil 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, pupils are up to date and aware of the risks.

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

Signed (Head Teacher):

Signed (e-Safety governor):

Appendix 6 **Inappropriate Activity Flowchart**



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

Appendix 7

Illegal Activity Flowchart