St. Peter & St. Paul CE Primary School, Burgh-le-Marsh

"Striving for excellence together in a caring Christian community."

RESPECT COMPASSION COURAGE

E-SAFETY POLICY

Responsibility: Governing Body

Approved on: 29/11/17

Signed: (Chair of Governors)

To be reviewed: Annually (September 2018) or earlier in the event of legislation changes, serious incident or named staff changes.

CONTENTS

SECTION 1: 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** – includes students, all staff, governing body, parents, volunteer helpers, those running extra-curricular activities*

Safeguarding is a serious matter. At our school we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, commonly 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 our website. All members of staff will sign as read and understood both the e-Safety policy and the Staff Acceptable Use Policy. Upon adoption and in light of subsequent modifications, a copy of this policy and the Student Acceptable Use Policy is to be sent home with existing students and to all new students thereafter. Upon return of the signed permission slip and acceptance of the terms and conditions, students will be permitted access to school technology including the Internet.

SECTION 2: ROLES & RESPONSIBILITIES

2.1 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 and 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.

- Designate specific governors 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 and receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

2.2 Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for e-Safety within our school. The day-to-day management of this may be delegated to a member of staff, the e-Safety Lead, 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 Lead has had appropriate CPD in order to undertake the day-to day duties.
- All e-Safety incidents are dealt with promptly and appropriately.

2.3 e-Safety Lead

The day-to-day duty of e-Safety Lead is currently devolved to David Hurdman (Acting Headteacher)
The e-Safety Lead 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 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 solution, progress tracking software) are fit for purpose through liaison with IT Technical Support.
- Make him/herself aware of any reporting function with technical e-Safety measures. E.g. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.

2.4 IT Technical Support Staff

Technical support staff are responsible for ensuring that the IT technical infrastructure is secure. IT Technical Support is currently provided by Education Lincs (191 Humberstone Avenue, Humberstone, DN36 4SZ, Tel 01472 813295). This will include at a minimum:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows/Apple 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 Lead and Headteacher.
- Passwords are applied correctly to all users regardless of age. Passwords for staff will be a minimum of 6 characters, contain a mix of upper and lower case letters and special characters (e.g. numbers). Staff passwords will be changed a minimum of every 42 days.
- The IT System Administrator password is managed by IT Technical Support and is to be changed on a regular basis.

2.5 All School 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 Lead, or in his/her absence to the Headteacher and is recorded on a Gold Incident Form. If unsure, the matter is to be raised with the e-Safety Lead or the Headteacher to make a decision.
- The reporting flowcharts contained within this e-Safety policy are fully understood.

2.6 All Students

The boundaries of use of IT equipment and services in our school are given in the Student Acceptable Use Policy. Any deviation or misuse of IT equipment or services will be dealt with in accordance with the behaviour policy.

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

2.7 Parents and Carers

Parents play the most important role in the development of their children. As such the school will support parents in the acquisition of the skills and knowledge they need to ensure the safety of children outside the school environment. Through parents' evenings, school newsletters and the website, the school will aid parents in keeping 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 (AUP) before any access is granted to school IT equipment or services.

SECTION 3: TECHNOLOGY

Our school currently uses a range of devices including desktop Windows PC's, Windows laptops, Nintendo Wii consoles, Nintendo DSi hand-held devices, Android devices, Apple MacBooks and iPads. In order to safeguard the student and in order to prevent loss of personal data we employ the following assistive technology:

3.1 Internet Filtering

We use a Meraki hardware filtering solution 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 Computing Subject Leader, e-Safety Lead and IT Support are responsible for ensuring that the filtering is appropriate and that any issues are brought to the attention of the Headteacher.

3.2 Email Filtering

We use a combination of System Center Endpoint Protection and Windows Defender software that prevents any infected email to be sent from the school, or to be received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

3.3 Encryption

School Windows devices which hold personal data (as defined by the current data protection legislation) are encrypted using BitLocker. No data is to leave the school on an un-encrypted device. Data transferred to 'cloud' storage must be encrypted during transfer and when stored remotely. Devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop or USB flash drives) is to be brought to the attention of the Headteacher immediately. 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.)

3.4 Passwords

Where configuration is possible, staff and students will be unable to access devices without a username and a password. Staff passwords will change at least every 42 days or if there has been a compromise, whichever is sooner. Automated prompts ensure that staff passwords are changed. Note that some devices (e.g. Nintendo DSi, Nintendo Wii consoles) are not password enabled, but do not contain personal data.

3.5 Anti-Virus

All capable devices will have anti-virus software (System Endpoint Protection and Windows Defender). This software will be updated at least weekly (usually daily) for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher or e-Safety Lead if there are any concerns. All SD cards and USB peripherals such as flash drives, external hard drives and digital cameras are scanned automatically for viruses before use.

3.6 System Back-up

The core IT system (server, personal data stored on the server) is completely backed up on at least a weekly basis through Redstore Back-up Solutions.

SECTION 4: SAFE USE

4.1 Internet

Use of the Internet in school is a privilege, not a right. Internet use will be granted to staff upon reading this e-Safety and the Staff Acceptable Use Policy. Internet use will be granted to students upon signing and returning their acceptance of the Student Acceptable Use Policy (also signed by parents on behalf of the student). All parents receive a letter explaining why internet use may be monitored in school (see section Letters and Documents)

4.2 Email

All staff are reminded that emails sent through school e-mail servers are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted. Students are permitted to use the school email system, and as such will be given their own email address. The email address will usually be made up of their first name and last name. (e.g. joe.bloggs@burghschool.org.uk)

4.3 Photos and videos

Digital media such as photos and videos are covered in the school's Photographic Policy. Permissions are reviewed by parents at the beginning of each academic year; non-return of confirmation of permission will not be assumed as acceptance.

4.4 Social Networking

There are many social networking services available. Our school supports the appropriate use 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 our school and have been appropriately risk assessed; should staff wish to use other social media, permission must first be sought via the e-Safety Lead who will advise the Headteacher for a decision to be made. Any new service will be risk assessed before use is permitted.

- Blogging – used by staff and students in school (e.g. primaryblogger.co.uk).
- TxtRound – used by the school as a broadcast service (see below).

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. Please refer to the school's Social Media Policy for further guidance. 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). Should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

4.5 Incidents

Any e-Safety incident is to be brought to the immediate attention of the e-Safety Lead, or in their absence the Headteacher. The e-Safety Lead will assist in taking the appropriate action to deal with the incident. e-Safety incidents should be recorded on a Gold Incident Form.

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

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

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

The e-Safety Lead, Headteacher and Governing Body are responsible for recommending and implementing a programme of training and awareness for the school year. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area, this should be brought to the attention of the Headteacher for further CPD.

St. Peter & St. Paul CE Primary School, Burgh-le-Marsh

"Striving for excellence together in a caring Christian community."

RESPECT COMPASSION COURAGE

ACCEPTABLE USE POLICY – STAFF

Note: All Internet and email activity in school or using school equipment is subject to monitoring.

Please read this policy in conjunction with the e-Safety Policy. Once you have read and understood both you must sign this policy sheet, returning the original and keeping a copy for yourself.

Internet access
Staff 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 intentionally offensive to colleagues. Inadvertent access must be treated as an e-Safety incident, reported to the e-Safety Lead and Gold Incident Form completed.

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 current Freedom of Information legislation.

Passwords
Staff should keep passwords private. Under no circumstances should a staff password be shared with another member of staff or student, or, unless there are exceptional circumstances, IT Support.

Data Protection and Encryption
If it is necessary to take work home, or off site, staff must ensure that devices (laptop, USB flash drive etc.) is encrypted. On no occasion should data concerning personal information be taken offsite or stored on an unencrypted device. Sensitive data transferred electronically must be encrypted during transfer and at point of remote storage. Refer to the school's Data Protection Policy and current legislation for further information.

Images and Videos
Staff must not upload onto any internet site or service images or videos of themselves, other staff or pupils without consent. This is applicable professionally (in school) or personally (e.g. staff outings). Staff must ensure that images and data are not uploaded automatically to personal accounts (e.g. as iCloud/Google Photos backups).

Personal Use of School IT
Staff are not permitted to use school IT equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries of personal use.

Use of Personal IT
Use of personal IT equipment is at the discretion of the Headteacher. Permission must be sought stating the reason for using personal equipment. A risk assessment will be carried out by IT Support and the e-Safety Lead. Staff must ensure that images and data are not uploaded automatically to personal accounts (e.g. as iCloud/Google Photos backups).

Viruses and other malware
Any virus outbreaks are to be reported to the IT Technical Support Helpdesk immediately, along with the name of the virus (if known) and actions taken by the school.

e-Safety
Like Health and Safety, e-Safety is the responsibility of everyone to everyone. As such staff will promote positive e-Safety messages in all use of IT with other members of staff and with students.

Social networking
Please refer to the separate Social Media Policy. In summary, staff using social networking for personal use should never undermine the school, its staff, parents or children.

Name : **Signed :** **Date :**

St. Peter & St. Paul CE Primary School, Burgh-le-Marsh

"Striving for excellence together in a caring Christian community."

RESPECT COMPASSION COURAGE

ACCEPTABLE USE POLICY – STUDENTS

RULES FOR GOOD ONLINE BEHAVIOUR

Note: All Internet and email activity in school or using school equipment may monitored.

I promise – to only use the school IT equipment 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 IT equipment. If I accidentally damage something I will tell my teacher.

I will not – share my password with anybody. 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 anybody asks me for personal information.

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

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

I understand – that some people on the Internet are not who they say they are and that 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 these rules there will be consequences of my actions and my parents will be told.

Signed (Parent):

Signed (Student):

Date:

St. Peter & St. Paul CE Primary School, Burgh-le-Marsh

"Striving for excellence together in a caring Christian community."

RESPECT COMPASSION COURAGE

INTERNET FILTERING AND MONITORING

INFORMATION FOR PARENTS

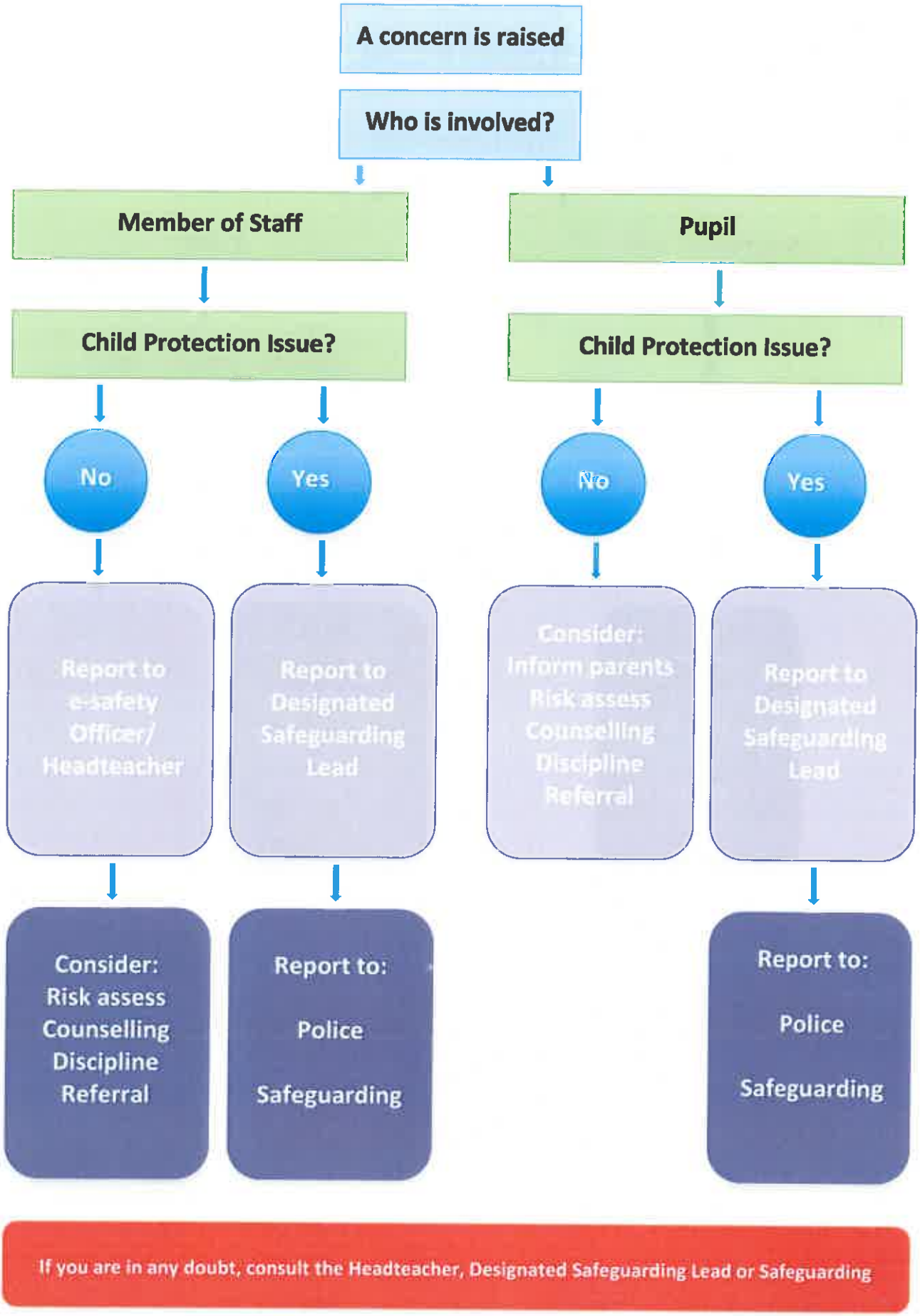
Use of the Internet in school is a vital part of the education of your child. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

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 sites such as this. We are able to do this using advanced software known as an Internet filter. At our school we currently use the Meraki filtering solution. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the user of specific equipment.

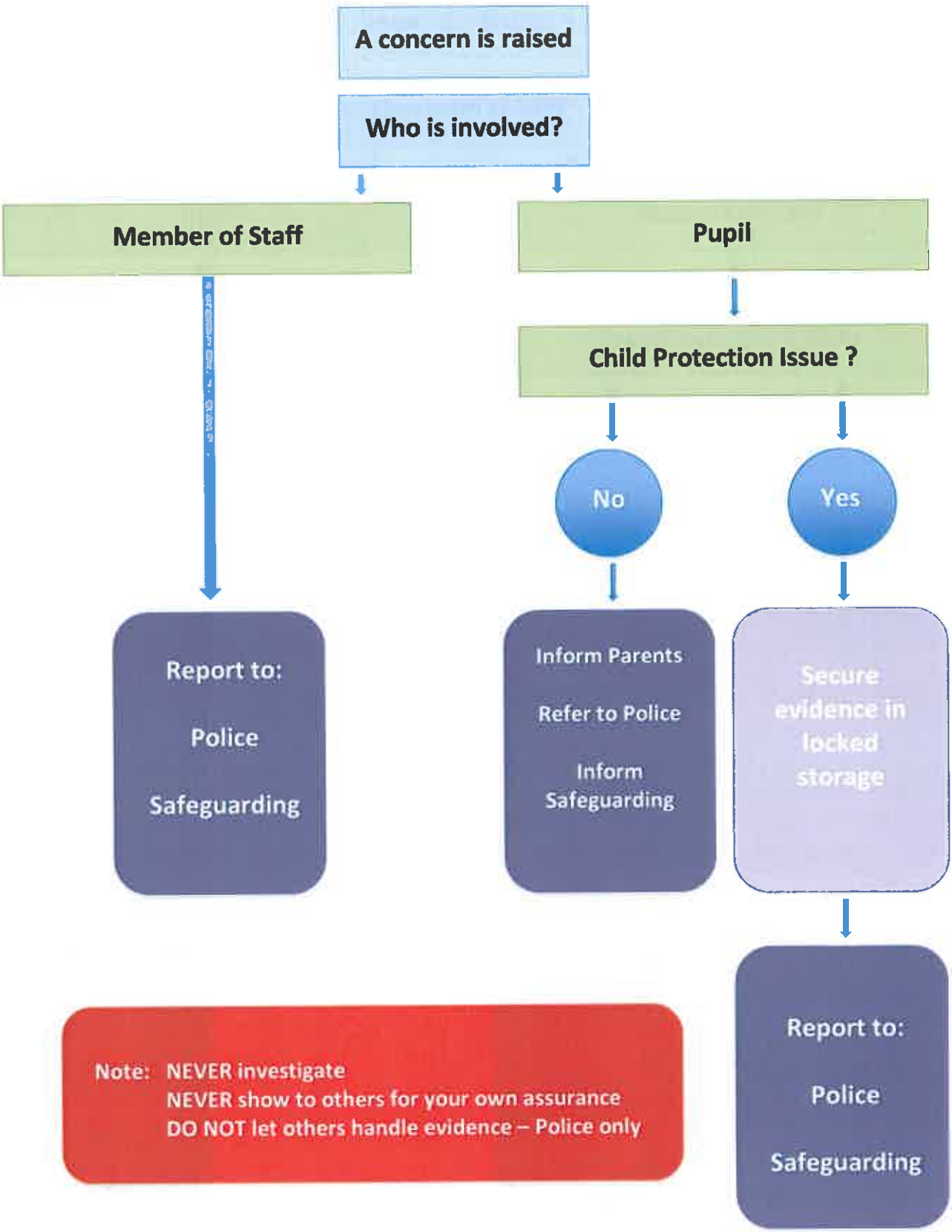
The software also allows us to monitor Internet use; the Internet filter keeps logs of which user has accessed what Internet sites, and when. Security and safeguarding of your child are of the utmost importance in our school. In order to ensure that there have been no attempts of inappropriate Internet 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.

Throughout the 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 them that we can monitor their activity. All children are given the opportunity to ask questions. If you have any questions or concerns please contact us.

APPENDIX 1: INAPPROPRIATE ACTIVITY FLOWCHART



APPENDIX 2: ILLEGAL ACTIVITY FLOWCHART



St. Peter and St. Paul C.E. Primary School, Burgh-le-Marsh

Appendix 3: RISK LOG

(Note: This is not an exhaustive list)

Activity	Risk	Likelihood	Impact	Score
Internet browsing	Access to inappropriate/illegal content - staff	1	3	3
Internet browsing	Access to inappropriate/illegal content - students	2	3	6
Blogging	Inappropriate comments	2	1	2
Blogging	Using copyright material	2	2	4
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

St. Peter and St. Paul C.E. Primary School, Burgh-le-Marsh
Appendix 4: FILTERING AND MONITORING

Introduction
Whilst sometimes seen as one of the more frustrating IT services in schools, Internet filtering is a particularly important aspect of e-Safety. When talking about an Internet filter there are two important aspects:

- **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.

Consider CCTV in a business premises; 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 customers and staff whilst in the building, 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?

Why do we Filter and Monitor?
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.
- Ensure (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 to:

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

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

Managing Expectations

It is the expectations of the user that is particularly important; this will include school staff, students and parents/guardians of the students. Consent is not a requirement, however you are required by law 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 actively monitor Internet activity, and neither do local authorities (remember, monitor is different to filter). Of course, some will disagree, 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

- 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.
- Statement in Acceptable Use Policy (AUP), e.g. "Users are reminded that Internet activity may be monitored". 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.

Summary

- Filtering is different to monitoring.
- Consent is not required, but users must be told if they are monitored or if there is the facility to monitor.
- Set user expectations; explain under what circumstances it may be a requirement to monitor.
- Ensure there is a good statement in your e-Safety Policy and users have been informed that Internet use "May be subject to monitoring" in the Acceptable Use Policy.
- Ensure parents are informed about the reason why monitoring may take place.