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

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

**RESPECT COMPASSION COURAGE**

# ONLINE SAFETY POLICY

Responsible: Governing Body

Agreed: January 2023

To be reviewed: Annually (or in the event of serious incident or legislation changes)

Reviewed: November 2023, November 2024

*Note: Throughout this policy Designated Safeguarding Lead (DSL) also refers to Deputy Designated Safeguarding Leads, even if not explicitly noted.*

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

**The 4 key categories of risk**

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

## 2. Legislation and guidance

This policy is based on the Department for Education’s (DfE’s) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

Teaching online safety in schools

Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff

[Relationships and sex education – see section 4]

Searching, screening and confiscation

It also refers to the DfE’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

## 3. Roles and responsibilities

### 3.1 The Governing Body

The Governing Body has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The Governing Body will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school’s IT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures

- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

### 3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### 3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.

The DSL and deputies take lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher, IT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 5 contains an example self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or Governing Body

This list is not intended to be exhaustive.

### 3.4 IT management (including security systems)

At our school, security is overseen by Education Lincs Ltd (Education Lincs Ltd, 191 Humberston Avenue, Humberston, DN36 4SZ, Office: 01472 813295, Support: 01472 813297). They report to the headteacher and are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's IT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that the school is supported with any online safety incidents in line with this policy
- Ensuring that the school is supported with any incidents of cyber-bullying in line with the school behaviour policy

This list is not intended to be exhaustive.

### 3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's IT systems and the internet (appendix 1), and ensuring that pupils follow the school's terms on acceptable use (appendix 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

### 3.6 Parents

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's IT systems and internet (appendices 1 and 2)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's IT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 1).

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

**All** schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour

- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website and Parenthub. This policy will also be shared with parents.

Online safety will also be covered during parents' evenings.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

The headteacher, and any member of staff authorised to do so by the headteacher (in our school this is the normally DSLs, including Deputy DSLs) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSLs.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's cooperation

**For further advice and guidance, staff must refer to the latest Government guidance 'Searching, Screening and Confiscation advice for schools' at https://www.gov.uk/government/publications/searching-screening-and-confiscation**

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

## 7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 to 3.

## 8. Pupils using mobile devices in school

Only Y6 children who walk home themselves may bring mobile devices into school. These must remain off the entire time they are on school premises. There is to be no use of personal mobile devices by children.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## 9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol). This is a system-wide applied policy.
- Ensuring their hard drive and portable devices are encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device. This is a system-wide applied policy.
- Making sure the device locks if left inactive for a period of time. This is a system-wide applied policy.
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software (fulfilled by IT support)
- Keeping operating systems up to date by always installing the latest updates (fulfilled by IT support)

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 1.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the headteacher or IT support.

## 10. How the school will respond to issues of misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies including behaviour, anti-bullying and acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's IT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the current HR policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## 11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL deputy DSLs will undertake child protection and safeguarding training in line with the LSCP pathway. They will also update their knowledge and skills on the subject of online safety at regular intervals.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

## 12. Monitoring arrangements

The school logs behaviour and safeguarding issues related to online safety. These are monitored by Senior Leaders and DSLs, including Deputy DSLs.

This policy will be reviewed at least annually. Reviews will consider and reflect the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

## 13. Links with other policies

This online safety policy should be read in conjunction with other policies, including:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- IT and internet acceptable use policy

# APPENDIX 1: ACCEPTABLE USE POLICY – STAFF, GOVERNORS & VISITORS

***Note 1: All Internet and email activity in school or using school equipment is subject to monitoring.***

*Please read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet (or complete the Google Form), returning the original and keeping a copy for yourself.*

**Internet access**
Staff (governors/visitors) 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 online safety incident, reported to the Online Safety/Safeguarding Lead and CPOMS incident form completed.

**Use of Email**
Staff (governors/visitors) are not permitted to use school email addresses for personal business. All email should be kept professional. Staff (governors/visitors) are reminded that school data, including emails, is open to Subject Access Requests under current Freedom of Information legislation.

**Passwords**
Staff (governors/visitors) should keep passwords private. Under no circumstances should a staff (visitor) password be shared with another member of staff (visitor) or pupil, 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 stored or taken offsite 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 (governors/visitors) 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 (governors/visitors) 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 (governors/visitors) 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 Online Safety Lead. Staff (governors/visitors) must ensure that images and data are not uploaded automatically to personal accounts (e.g. as iCloud/Google Drive 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.

**Online Safety**
Like Safeguarding and Health & Safety, Online Safety is the responsibility of everyone to everyone. As such staff (governors/visitors) will promote positive Online Safety messages in all use of IT with other members of staff and with pupils.

**Social networking**
Please refer to the separate Social Media Policy and Local Authority policies. In summary, staff (governors/visitors) using social networking for personal use should never undermine the school, its staff, parents or pupils.

# APPENDIX 2: ACCEPTABLE USE POLICY – PUPILS

## 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):** ____________________________ **Date:** ___________________________

**Signed (Pupil):** ____________________________ **Date:** ____________________________

## INTERNET FILTERING AND MONITORING

## INFORMATION FOR PARENTS

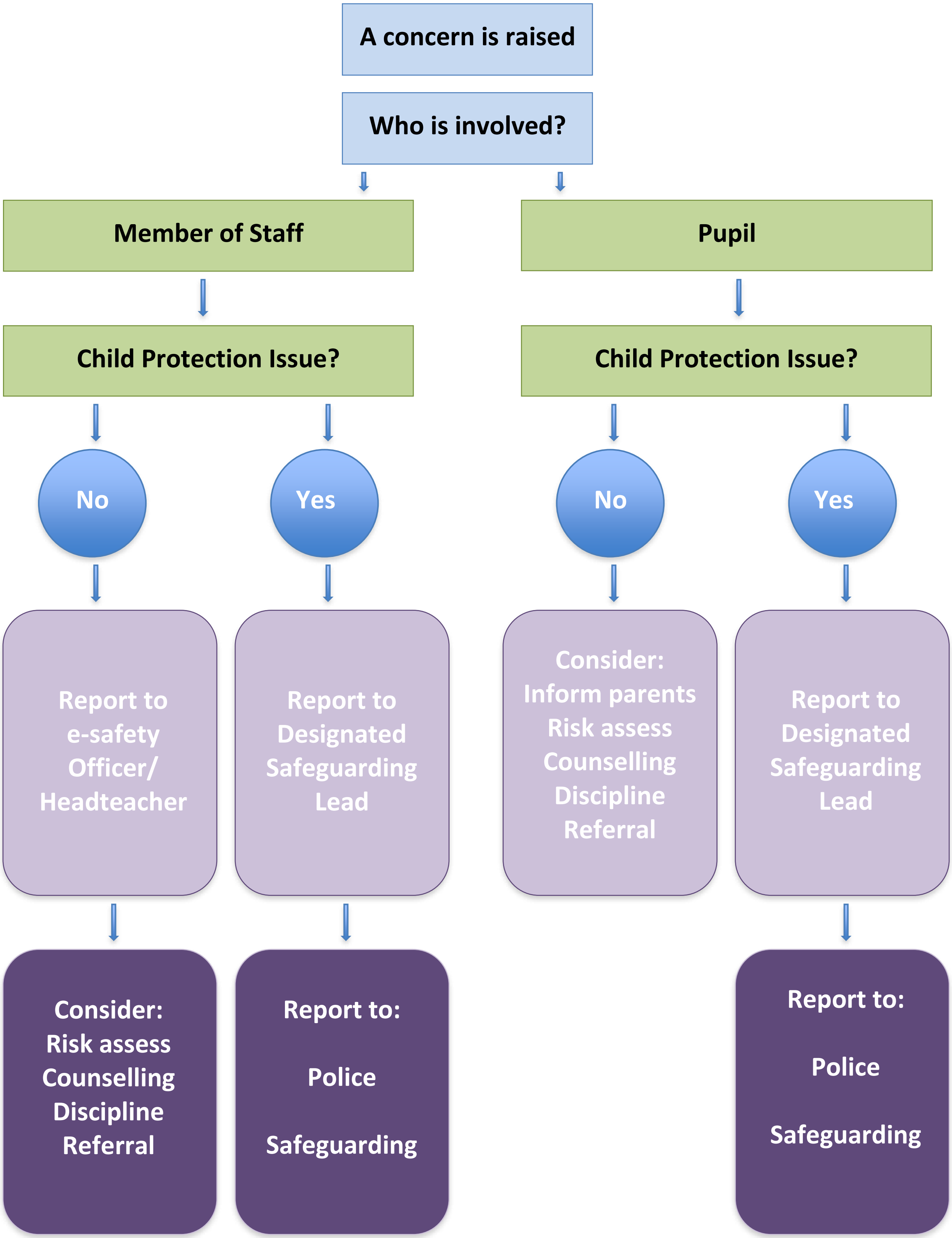
Use of the Internet in school is a vital part of the education of your child. Our school makes extensive use of the Internet in order to enhance their learning and provide facilities for research, collaboration and communication.

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 Cisco 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 3: INAPPROPRIATE ACTIVITY FLOWCHART



A concern is raised

Who is involved?

Member of Staff

Child Protection Issue?

No

Report to e-safety Officer/ Headteacher

Consider:
Risk assess
Counselling
Discipline
Referral

Yes

Report to Designated Safeguarding Lead

Report to:

Police

Safeguarding

Pupil

Child Protection Issue?

No

Consider:
Inform parents
Risk assess
Counselling
Discipline
Referral

Yes

Report to Designated Safeguarding Lead

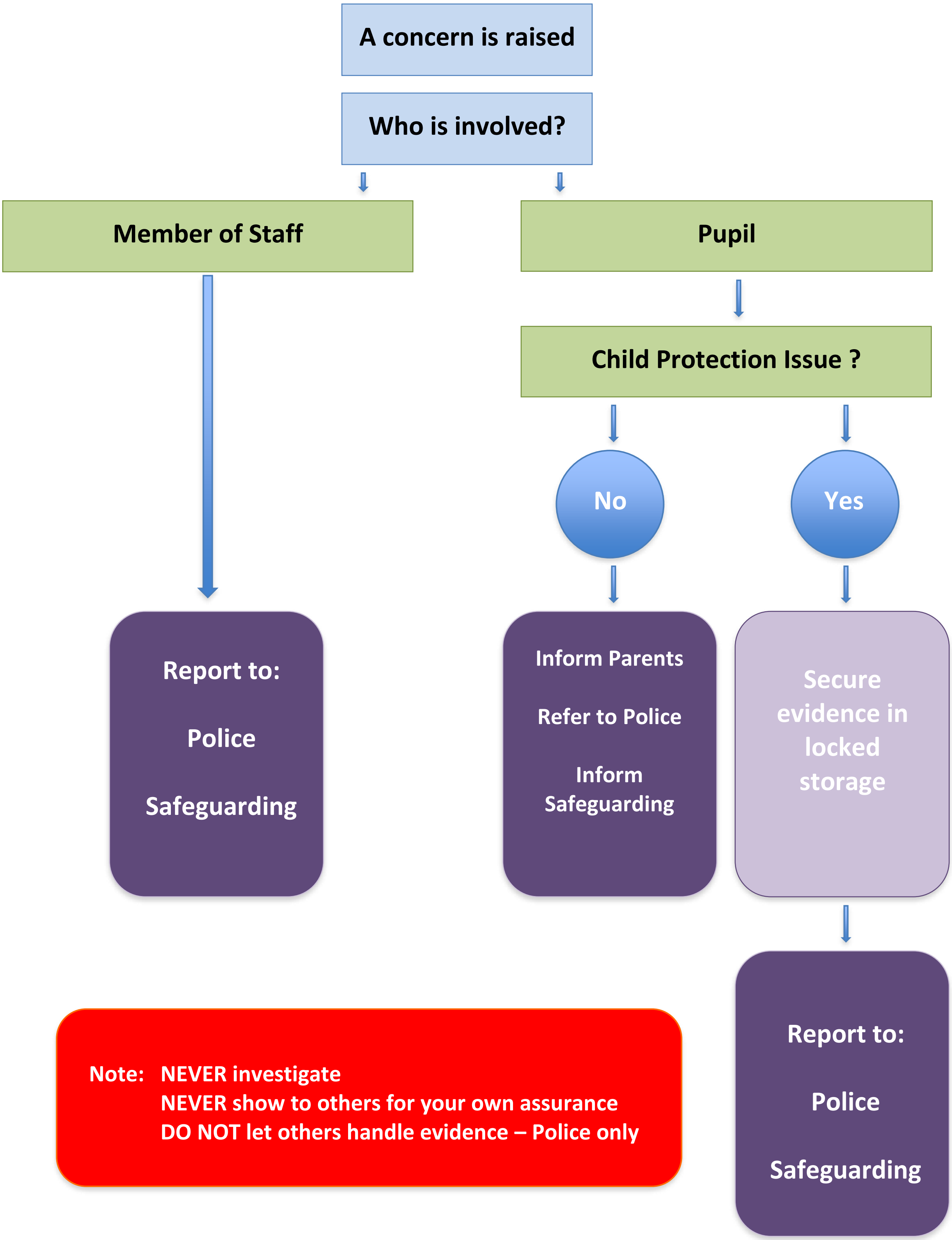
Report to:

Police

Safeguarding

**If you are in any doubt, consult the Headteacher, Designated Safeguarding Lead or Safeguarding**

# APPENDIX 4: ILLEGAL ACTIVITY FLOWCHART



A concern is raised

Who is involved?

Member of Staff

Report to:

Police

Safeguarding

Pupil

Child Protection Issue ?

No

Inform Parents

Refer to Police

Inform Safeguarding

Yes

Secure evidence in locked storage

Report to:

Police

Safeguarding

Note: NEVER investigate
NEVER show to others for your own assurance
DO NOT let others handle evidence – Police only

# APPENDIX 5: ONLINE SAFETY TRAINING NEEDS – SELF-AUDIT FOR STAFF

| ONLINE SAFETY TRAINING NEEDS AUDIT | |
|---|---|
| **Name of staff member/volunteer:**<br>**Role:** | **Date**: |
| **Question** | **Yes/No (add comments if necessary)** |
| Do you know the name of the person who has lead responsibility for online safety in school? | |
| Are you aware of the ways pupils can abuse their peers online? | |
| Do you know what you must do if a pupil approaches you with a concern or issue? | |
| Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors? | |
| Are you familiar with the school's acceptable use agreement for pupils and parents? | |
| Do you regularly change your password for accessing the school's ICT systems? | |
| Are you familiar with the school's approach to tackling cyber-bullying? | |
| Are there any areas of online safety in which you would like training/further training? | |