Policy Statement for

Online Safety & Acceptable Use

Other related policies to cross reference and refer: Behaviour and Anti-Bullying, Safeguarding, Staff Behaviour, Whistleblowing

Change History	Summary of Key Changes
Jan 2017	Updated the term ESafety to online safety throughout
Feb 2019	Changed incident reporting form to work on line and linked to bullying incident form; updated staff user acceptance policy; clarified use of mobile phones and messaging in school; clarified encryption of sensitive emails; added section on Breaches of the policy to main body and staff user acceptance policy
Mar 2020	Changes to names and KCSIE references. Banning the use of mobile phones in school by children although they may be kept in the office if required for personal communication. Removed reference to Twitter
Jan 2021	Reference made to remote learning due to COVID 19 pandemic

Table of Contents

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Online safeguarding is an area that is constantly evolving.

We use technology and the internet extensively across all areas of the curriculum and we do all that is possible to ensure children are protected.

Purpose and Aims

The primary purpose of this policy is:

- 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 children or liability to the school.
- To keep children safe from harm by directly linking online safety to the school's Safeguarding and Child Protection Policy.

This policy is available for anybody to read on the school website; upon review all members of staff will sign as read and understood both the Online Safety Policy and the Staff Acceptable Use Policy. A copy of this policy and the Children Acceptable Use Policy will be sent home assuming agreement with new children at the beginning of the school year with a non-consent slip. Upon return of a signed non-consent slip, children will not be permitted access to school technology to use the Internet and alternative provision will be made during computing lessons.

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

Users - refers to staff, governing body, school volunteers, children and any other person working in or on behalf of the school, including contractors

Parents – any adult with a legal responsibility for the child 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 – children, all staff, governing body, parents.

Online Safety Officer - the individual responsible for managing and overseeing Online Safety in school.

Online Safety officer & Designated Safeguarding Lead: Liz Geller
Online Safety Governor: Peter Holmes
Deputy Designated Safeguarding Leads: Mark Davis, Sarah Edwards
Computing Subject Leader: Liz Geller

This policy has been developed by the Online Safety Officer (who is also the Head Teacher) and the Designated Online Safety Governor in consultation with the governing body and staff. The policy is

available to staff, governors, volunteers, parents and carers through the school website, as a hard copy upon request at the school office and for staff in a central intranet folder.

The policy should be read alongside the school's policy on Safeguarding and Child Protection and shares its policy aims;

- **To make sure our school is a place where children feel safe, are encouraged to talk, and are listened to.**
- **To make sure children know that there are adults in the school who they can talk to if they are worried.**
- **To help children to develop the skills they need to recognise and stay safe from abuse (including online abuse).**
- **To guide use of online learning in the event of the school being closed. (see Annex H of the Safeguarding Policy)**

Any concerns regarding Online Safety should be directed immediately to the Online Safety Officer, or where a child may be at risk to a Designated Safeguarding Officer.

This policy will be reviewed on an annual basis or in response to an Online Safety incident, whichever is sooner.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy at least annually and in response to any Online Safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure Online Safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of Online Safety at the school who will:
  - Keep up to date with emerging risks and threats through technology use.
  - Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.
  - establish the effectiveness (or not) of Online Safety training and awareness in the school.
  - to recommend further initiatives for Online Safety training and awareness at the school.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for Online Safety within our school and for any remote learning. The day-to-day management of this will be the responsibility of the Headteacher.

They will ensure that:

- Online Safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. children, all staff, senior leadership team and governing body, parents.
- The designated Online Safety Officer has had appropriate CPD in order to undertake the day to day duties.
- All Online Safety incidents are dealt with promptly and appropriately.

Online Safety Officer

The Online Safety Officer will:

- Keep up to date with the latest risks to children whilst using technology: familiarise themselves with the latest research and available resources for school and home use.
- Review this policy regularly and deal with any matters arising in discussion with the Headteacher.
- Advise the governing body on all Online Safety matters.
- Engage with parents and the school community on Online 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 Online Safety incident log (held on the school intranet site); ensure staff know what to report and ensure the appropriate audit trail is in place.
- Ensure any technical Online Safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or Computing Technical Support.
- Make themselves aware of any reporting function with technical Online Safety measures, i.e. internet filtering reporting function; liaise with the responsible governor to decide on what reports may be appropriate for viewing.

Designated Safeguarding Lead

The Designated Safeguarding Lead will:

- be trained in Online Safety issues
- be aware of the potential for serious child protection / safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - online-bullying

Computing Technical Support Staff

Technical support staff (internal and contractors) are responsible for ensuring that:

- The IT technical infrastructure is secure; this will include at a minimum:
    - Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
    - Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
    - Any Online 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 Online Safety officer/Headteacher.
    - Passwords are applied correctly to all adult users

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any Online Safety incident or potential Online Safety incident is reported to the Online Safety Officer/Head Teacher (and an Online Safety Incident report is made).
- The reporting flowcharts contained within this Online Safety policy are fully understood.

All Children

The boundaries of use of computing equipment and services in this school are given in the **Children Acceptable Use Policy**; any deviation or misuse of computing equipment or services will be dealt with in accordance with our policies for **Behaviour, Anti Bullying & Hate, Safeguarding & Child Protection**.

Online Safety is embedded into our curriculum through lessons, assemblies and discussion; children will be given the appropriate advice and guidance by staff. Similarly all children will be fully aware how they can report areas of concern whilst at school or outside of school.

Parents

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 and school newsletters the school will keep parents up to date with new and emerging Online Safety risks, and will involve parents in strategies to ensure that children are empowered. It is recommended that parents use the internet at home with their child, develop a similar set of rules and invest in appropriate security software. During any closure related to COVID 19, parents will need to ensure their children are kept safe during any home use of the internet for remote learning.

Parents must also understand the school needs to have rules in place to ensure that their child can be properly safeguarded. As such parents will receive the **Children's Acceptable Use Policy** and are able to deny permission for their children to access the internet on school computing equipment.

Security

Nailsworth Church of England Primary School have revised this policy in line with *Keeping Children Safe in Education 2020* to ensure that appropriate filters and appropriate monitoring systems are in place for all devices so that children will not be able to access harmful or inappropriate material from the school IT system.

Nailsworth Church of England Primary School uses a range of devices including PCs, laptops and tablets. In order to safeguard the children and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – we use RM SafetyNet Plus supplied by SWGfL 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 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 RM EasyMail security that prevents any infected email being sent from the school, or received by 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 – Encryption is used when sending and receiving sensitive information from other professional services/people using INGRESS. The Headteacher and SENCO have INGRESS accounts. Teachers who need to send sensitive information should request the Headteacher or SENCO to forward the information on their behalf.

All sensitive information is held on the schools OneDrive intranet, only accessible on a need to know basis, controlled by the Headteacher. Staff are requested to regularly use the FREE UP SPACE option in OneDrive which forces documents to be held in the intranet and not on local devices, such as laptops.

Passwords – all staff will be unable to access any device containing confidential pupil or other data without a unique username and password. IT Support will be responsible for ensuring that passwords are changed regularly.

Anti-Virus – All capable devices will have anti-virus software. This software will be updated 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. All USB peripherals, such as key drives, are to be scanned for viruses before use.

Safe Acceptable Use

(please refer to Appendix 1 and 2)

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing the **Staff Acceptable Use Policy**; to children, unless **non-parental consent** is received

following distribution of the **Children Acceptable Use Policy**. Children will not pursue internet research without staff supervision and the free use of search engines is not permitted.

Email – All staff are reminded that emails are subject to Freedom of Information requests and subject to scrutiny by the school's filtering provider. Staff should use school supplied emails for all school correspondence. Personal email addresses are not to be except in an emergency. Individual staff email addresses set up through the school are to be used for professional work-based emails only. Emails of a personal nature are not permitted. Children do not have their own individual email addresses and use a class email when needed, which is managed by the class teacher.

Photos and videos – Digital media such as photos and videos are covered in the **Use of Photographic Images consent form**, and is re-iterated here for clarity. All parents must sign a photo/video release slip; non-return of the permission slip will not be assumed as acceptance. Any images of children will not be labeled with their names and will only appear on the website if parents have agreed to this.

Social Networking – Social media services used by the school are limited to Facebook for parent information, used only by authorized staff with private settings and within a closed group, and Blogger for Residential trips, which is by invite only and not open to search engines. Our website enables a blog facility. This is controlled by staff and all posts created by pupils will need to be approved before they can be posted online. If staff wish to use other social media, permission must first be sought via the Online Safety Officer/Headteacher for a decision to be made. The Social Media policy should be referred to.

Notice and Take Down procedure – 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 online safety incident is to be brought to the immediate attention of the Online Safety Officer, (Headteacher) or in his absence, one of the Deputy Safeguarding Officers. The Online Safety Officer will take the appropriate action to deal with the incident and to fill out an Online Safety Incident Log (Appendix 7).

Training

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. The Online Safety Officer keeps up to date with the latest risks to children whilst using technology ensuring that he is familiar with the latest research and available resources for both school and home use. The Online Safety Officer disseminates relevant information to all staff as it arises through weekly staff meetings. The school has an annual programme of training which is suitable to the audience and any additional training found necessary as a result of Online Safety incidents or other instigators.

The Gloucestershire County Council Online Safety Officer is responsible for recommending a programme of training and awareness for the school year to the Headteacher and the designated 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.

Curriculum

Making sure that children do not access 'inappropriate' content is essential but only part of the bigger picture; online safety includes educating children about and protecting them from online abuse, online grooming, privacy violations, cyber bullying, sexting and also associated mental health issues such as anxiety, depression and lack of sleep.

Online Safety for children 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 the risks, as part of the children's learning. Progressive, discrete online safety lessons are taught throughout the school with additional emphasis during Anti-bullying, Healthy Living or Online Safety initiatives. In year four, children watch a play about internet safety, "IN THE NET".

Through our planned PSHE education programme and school values, we underpin safe learning that is age appropriate but with an awareness that many children may be experiencing or exposed to online content that is intended for older children or adults. This will include work on:

- communication
- understanding healthy relationships, including trust
- understanding and respecting the concept of genuine consent
- understanding and respecting self-image and identity
- understanding our rights (especially our collective right to *be* safe and to *feel* safe)
- recognising abusive and coercive language and behaviours
- accepting our responsibilities (especially our responsibility to respect others' trust and protect their right to be physically, emotionally and socially safe)

Extra lessons are to be taught in response to Online Safety incidents or changes.

School Action in Response to National Online Safety Concerns

The school is registered with National Online Safety and receive regular updates and notifications of current issues and concerns. Any high level threats are instantly notified to all staff and where appropriate we talk to the children and make parents aware.

The Online Safety Officer will take the appropriate action to deal with the incident and to fill out an Online Safety Incident Log (Appendix 7).

Children with Special Educational Needs and Disabilities (SEND)

We acknowledge that children with **special educational needs and disabilities (SEND)** can face additional safeguarding challenges online and may need extra support and guidance around being safe online. Teaching is differentiated and SEND trained Teaching Assistants provide additional support to children who may be more vulnerable. Particular vulnerability may exist around being:

- disproportionally impacted by behaviours such as online bullying, grooming and radicalisation without outwardly showing any signs;
- and communication barriers and difficulties.

Peer on Peer Online Abuse

"Bullying that happens online, using social networks, games and mobile phones, is often called cyberbullying. A child can feel like there's no escape because it can happen wherever they are, at any time of day or night."
https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/

Peer on Peer online abuse can take the form of cyber bullying, sexting, sexual harassment or stalking and should never be ignored. If any member of staff, child or parent/carer suspects a child of inappropriate behavior online, the Designated Safeguarding Officer and the Online Safety Officer must be informed and safeguarding procedures will be followed. These procedures are detailed in the Safeguarding & Child Protection Policy. The Anti-bullying & Hate Policy should also be referred to.

Raising Online Safety Concerns

Staff who have an online safety concern, related to or involving a child, should speak to the Online Safety Officer who will complete an Online Safety Incident Log and take further action, as necessary. Where a child is suspected to be a perpetrator or a victim of peer on peer online abuse, safeguarding procedures must be followed and the designated safeguarding lead informed.

Online safety concerns related to or involving a member of staff should be reported in the first instance to the Online Safety Officer who will complete an Online Safety Incident Log and take further action, as necessary.

Parents/carers who have an online safety concern, related to the school, staff or other pupils in the school, should contact the Online Safety Officer who will complete an Online Safety Incident Log and take further action, as necessary.

Children who are worried about the way someone has been communicating with them online or have an online safety concern, should talk to or write a note to their class teacher who will complete an Online Safety Incident Log with them and notify the Online Safety Officer to take further action, as necessary.

Online safety concerns can also be reported to:

- The police CEOP (Child Exploitation and Online Protection) command via an easy to use web form: https://www.ceop.police.uk/safety-centre/
- Anonymously to The Front Door (the Children and Families Helpdesk) on 01452 426565

If there is a concern that a child is at immediate risk of harm, call the police on 999.

Breaches of the Policy

(please refer to Appendix 8 and 9)

Staff and volunteers, including contracted staff

Any breaches of this policy will be investigated and may lead to disciplinary action being taken against the staff member/s involved in line with the Staff Behaviour Code and Procedures policy and the Whistleblowing policy.

Breaches of this policy may include, but not limited to, breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school liable to third parties, or that involve allegations of online abuse staff on staff.

Contracted providers of the school must inform the school immediately of any breaches of this policy by their employees whilst contracted by the school so that appropriate action can be taken to protect confidential information, limit the damage to the reputation of the school and safeguard the children of the school. Any action against breaches should be dealt with in accordance with the contractor's own internal disciplinary procedures.

Pupils

Any breaches to this policy will be investigated and dealt with through the school's Behaviour policy and other related policies.

If you are in doubt about any of the above, please seek advice from the Online Safety Officer.

Appendix 1 - Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults				Pupils			
Communication Technologies	Allowed	Allowed at certain times with conditions applied	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times with conditions applied	Allowed with staff permission	Not allowed
Mobile phones may be brought to school*	X				X*			
Use of mobile phones in lessons for personal use				X				X
Use of mobile phones in lessons to support lesson enquiries	X							X
Use of mobile phones in social time	X							X
Taking photos on mobile phones or other camera devices		X					X	
Use of hand held devices eg PDAs, PSPs	X							X
Use of personal email addresses in school, or on school network	X							X
Use of school email for personal emails				X				X
Use of chat rooms / facilities				X				X
Use of instant messaging for personal use				X				X
Use of instant messaging for school use	X				X			
Use of social networking sites		X						X
Use of blogs/video-logs			X				X	

* Children may bring mobile phones into school with specific agreement between parents, teachers and the headteacher. They are kept in the office and are not accessible until home time. This is to ensure children who walk home have a way of communicating with their parents, if necessary.

When using communication technologies the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff should therefore use the school email service to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Users must report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to the to the Online Safety officer immediately and must not respond to any such email. The Online Safety Officer should refer to the Safeguarding & Child Protection Policy, Behaviour Policy, Staff Behaviour Code and Procedures and/or Anti-Bullying & Hate Policy for further guidance.
- Any digital communication between staff and parents / carers (email, Twitter, Facebook, etc) must be professional in tone and content. Personal email addresses or public chat / social networking programmes must not be used for these communications, with the exception of Facebook Families of Nailsworth Primary closed group page where authorized staff in their professional capacity can communicate using Facebook Messenger. Text messaging must only be carried out using the school text messaging service (teachers2parents).
- Whole class or group email addresses and nailsworthschool.org website logins will be used at KS1 and KS2 for educational use.
- Pupils should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- Photos may be taken on the school camera and the memory stick must remain in school at all times. Photos should be stored on school intranet only and deleted off portable laptops within 24 hours of uploading from a camera. If a staff mobile phone is used for digital media, the media must be removed as soon as possible, by the end of the next working day at the latest.
- Blogging and video-logging may be carried out as part of a supervised activity through Blogger and the school website only. All blogs/v-logs are controlled and have to be approved by the staff member in charge before uploading is possible to the internet.

Appendix 2 - Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts computer and certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	child sexual abuse images					X
	promotion or conduct of illegal acts, eg under the child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion & hinders others in their use of the internet					X	
On-line gaming (educational)			X			
On-line gaming (non educational) no violent/fighting games				X		
On-line gambling					X	
On-line shopping / e-commerce for school procurement only		X				
File sharing				X		
Use of social networking sites				X		

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Use of video broadcasting (eg YouTube) for educational clips only		X			

Appendix 3 - Monitoring

- All staff, children and parents of children 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.
- Staff must understand why monitoring is important, be allowed to voice any concerns and set their expectations of how the data can be used.
- A letter is sent home to parents, explaining that the Internet activity may be monitored, and why, to be distributed alongside the **Children's Acceptable Use Policy**.

  Note: users must be informed of monitoring, but consent is not required.

Appendix 4 – Acceptable Use Policy: Staff

Acceptable Use Policy – Staff

Note: All Internet and email activity is subject to monitoring

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both you must sign this policy sheet and return to the school office.

General Security – You must be vigilant with security of passwords and the use of IT equipment. Staff computers should be screen locked whenever you leave them unattended.

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 Online Safety incident, reported to the Online Safety officer and an incident sheet completed.

Social networking – Social networking is allowed in school in accordance with the Online Safety policy only. Staff using social networking for personal use should never undermine the school, its staff, parents or children and staff should not identify themselves with the school except through professional sites like LinkedIn.

Staff should not become "friends" with or "followers" of parents or pupils on personal social networks, nor make contact with them through social networking sites. Staff must decline "friend requests" from pupils.

Use of Email – Emails are subject to Freedom of Information requests and subject to scrutiny by the school's filtering provider. Staff should use school supplied emails for all school correspondence. Personal email addresses are not to be used except in an emergency. Individual staff email addresses set up through the school are to be used for professional work-based emails only. Emails of a personal nature are not permitted. Children do not have their own individual email addresses and use a class email when needed, which is managed by the class teacher.

Passwords - You must keep passwords private. There is no occasion when a password needs to be shared with another member of staff or children, or IT support. You must comply with IT support if a request is made to change a password. Where a password needs to be created by staff, e.g. for editing the website, the password must be recognized as 'strong' and should be changed regularly. Children should never edit the website using your login details. You should ensure that you log out of the website when they have finished editing.

Data Protection – At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse. If it is necessary for you to take work home, or off site, you should ensure that your device (laptop, USB pendrive etc.) is password protected. On no occasion should data concerning confidential pupil information be stored locally on an unencrypted device. You should try to avoid saving confidential information locally at all, however if confidential information has to be downloaded, the device should be cleared as soon as possible, by the end of the next working day at the latest. You must ensure that you are properly "logged-off" at the end of any session in which they are using personal data.

Personal Use of School computing - You are not permitted to use computing equipment for personal use unless specific permission has been given from the Headteacher who will set the boundaries for 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 computing - Use of personal computing equipment is at the discretion of the Headteacher and must comply with the Online Safety policy. 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 Officer.

Viruses and other malware - Any virus outbreaks are to be reported to Online Safety Officer for appropriate escalation as soon as it is practical to do so, along with the name of the virus (if known) and actions taken by the school.

Online Safety – Like health and safety, Online Safety is the responsibility of everyone to everyone. As such you will promote positive Online Safety messages in all use of computing whether you are with other members of staff or with children.

Breaches of the Policy - Any breaches of this policy may be investigated and lead to disciplinary action being taken against the staff member/s involved in line with the School Disciplinary Policy and Procedure. A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of the school or any illegal acts or acts that render the school liable to third parties may result in disciplinary action or dismissal. **If you are in doubt about any of the above, please seek advice.**

NAME :

SIGNATURE : **DATE :**

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Appendix 5 – Use of Internet Letter to Parents/Guardians

Dear Parent/Guardian,

Use of the Internet

Use of the internet in school is a vital part of the education of your son/daughter. Our school makes good 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. This filter categorises websites in accordance with their content; the school allows or denies these categories dependent upon the age of the child, through SWGfL – South West Grid for Learning.

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. If you would like information or guidance to support safe internet usage at home, you may find our Protecting Children Online webpage useful:
https://www.nailsworthschool.org.uk/index.php/protecting-children-online/

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 them that we can 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 me.

We would like you to discuss the Charter of Good Online Behaviour (see overleaf) with your child. We realise that some of these items will not apply to our youngest children, but we want you to be aware of what we consider to be 'Acceptable Use'. We also ask that you accept responsibility for setting standards for your child to follow when selecting, sharing and exploring information and media at home.

If you are **not** happy for your child to use the internet in school to support their education, please return the reply slip below. Unless a non-consent reply slip is received, we assume your agreement to allow your child to use school computing equipment to access the internet.

Yours sincerely

Elizabeth Gellar
Headteacher and Online Safety Officer

✂----------

Non-consent for use of the Internet

I have read this letter and the Charter of Good Online Behaviour. I **do not** provide consent for my child to use school computing equipment to access the internet in school.

Name of Child – Name of Parent/Guardian –

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Signature - Date -

Appendix 6 – Acceptable Use Policy: Children

Acceptable Use Policy – Children

Our Charter of Good Online Behaviour

Note: All Internet and email activity is subject to monitoring

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

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

I will not – share personal information or images 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 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 there will be consequences of my actions and my parents will be told.

Appendix 7 - Online Safety Incident Log

Online Safety Incident Record

Date of Report:
Name of person reporting the incident(s):
Details of person/location of incident(s):

Summary of incidents:
Website □ Social Media □ Texting □

Is it related to bullying behaviour: Yes/No
Has a bullying incident been raised: Yes/No

Other notes connected to the incident and any previous unknown incidents:

Checklist:

Check for incidents involving same person	□	Follow up date set	□
Notified parents/carers	□	Action agreed with person involved	□
Discussion with group of people involved	□	Changed filtering of website	□

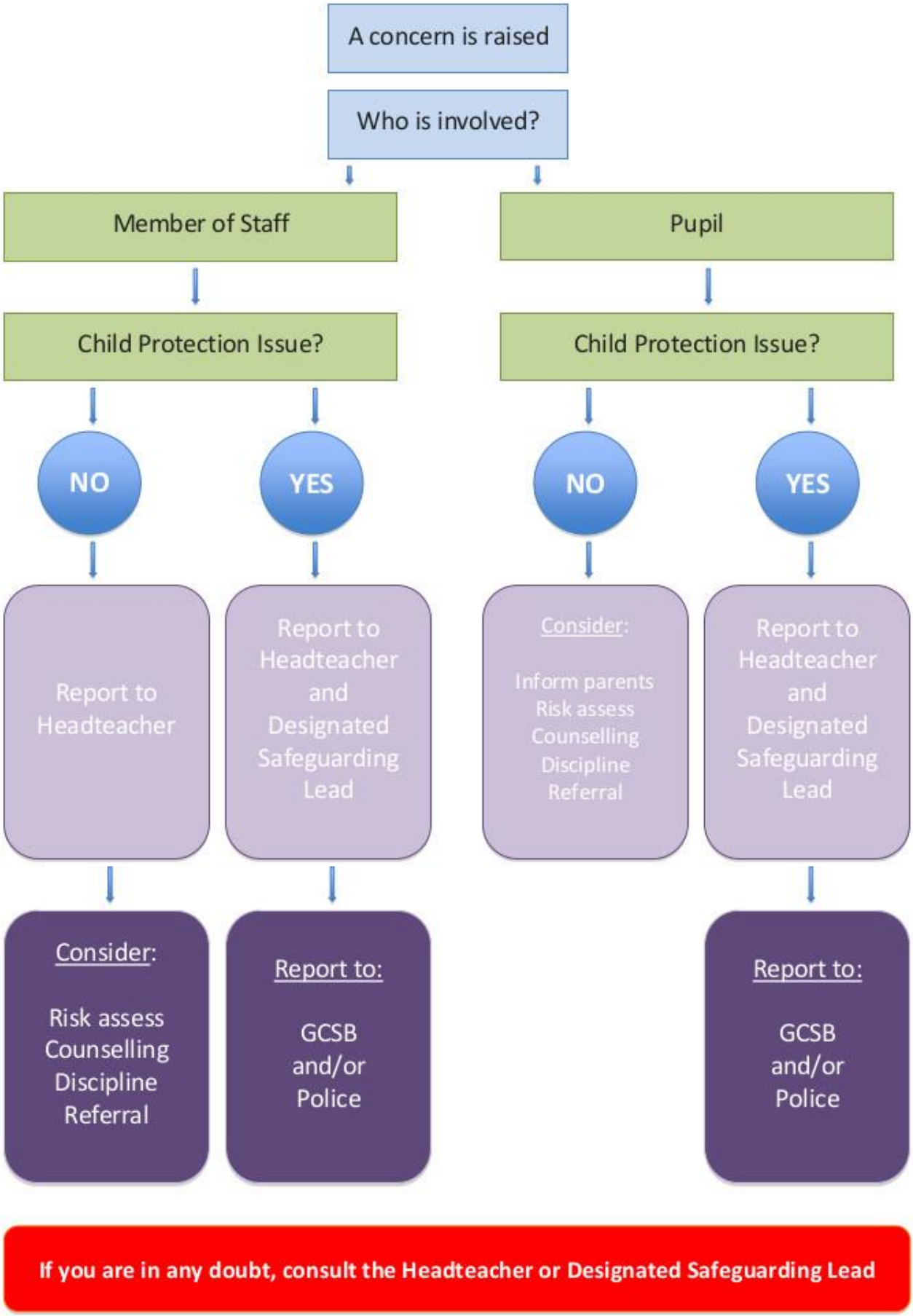
Details of agreed actions with people involved (including parents if relevant):

Follow up review outcomes:
Has the incident/occurrence stopped? Yes/No

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Appendix 8 – Inappropriate Activity Flowchart

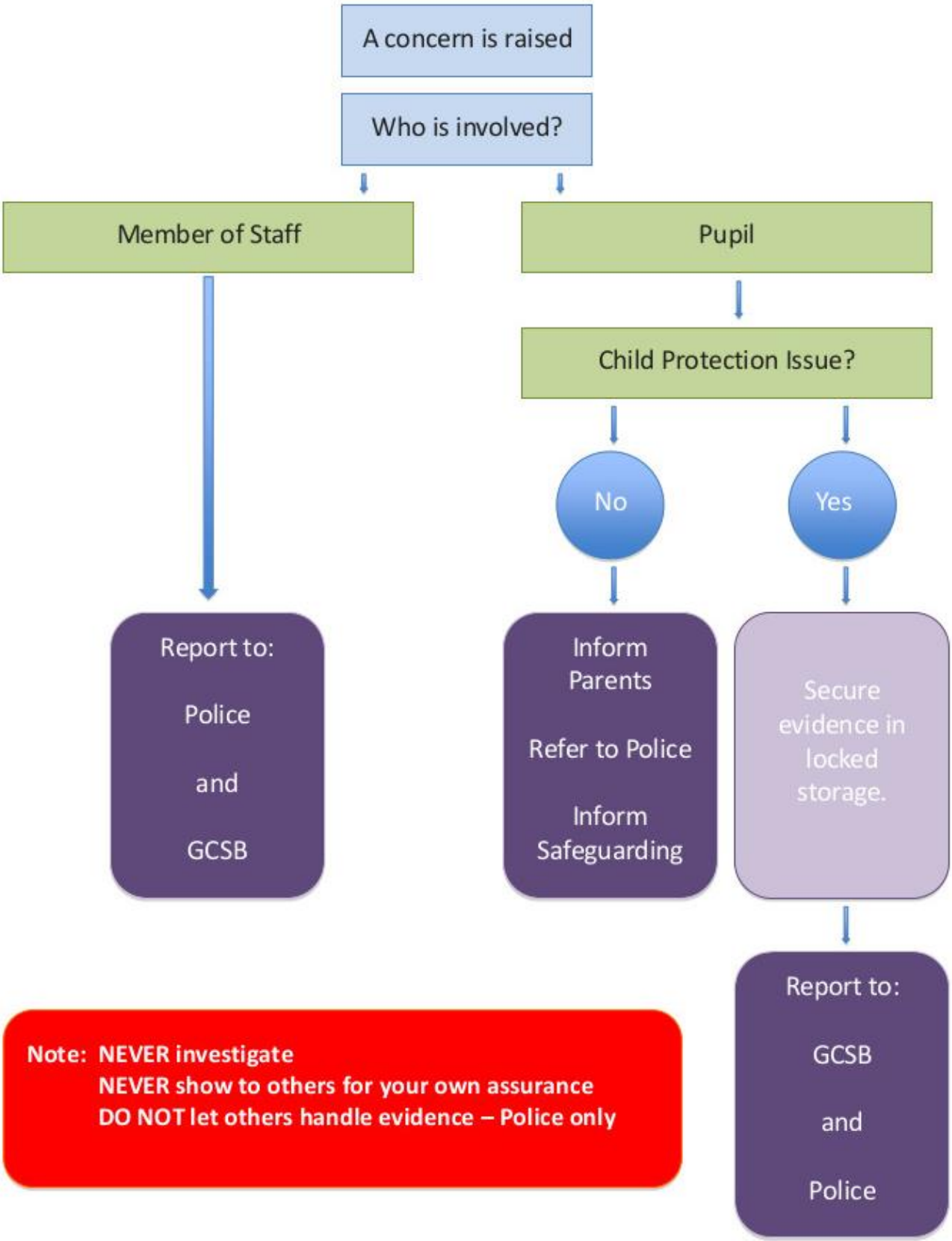
Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes



Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes

Appendix 9 – Illegal Activity Flowchart

Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes



Owner:	Standards Committee	Delegated To	Safeguarding Governor
Review Frequency	Annual (or in response to incidents)	Updated	Jan 2021
		Date ratified by Governing Body	Jan 2021
Version	4.0	Next Review	Jan 2022
Review Author	E Gellar / P Holmes	Published on Website	Yes