Online Safety Policy

Katherine Semar Infant and Junior Schools

Approved by:	Julie Puxley (headteacher)	**Date:** February 2023
Last reviewed on:	February 2023	
Next review due by:	February 2025	

Contents

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
- 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.

3. Roles and responsibilities

3.1 The governing board

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

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguard lead and deputy safeguarding leads.

A member of the governing body, who is also the safeguarding governor will be made aware of anonymised online safety incidents.

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 ICT systems and the internet (appendix 3),
- 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 (also the DSL) is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school, though the day-to-day responsibility for online safety will be designated to one of the deputy DSLs.

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.

One of the deputy DSLs (also the computing subject leader) takes 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, the SAT ICT 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 (see appendix 4) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged (see appendix 4) and dealt with appropriately in line with the school behaviour policy.
- Updating and arranging the delivery or delivering staff training on online safety.
- Liaising with and managing the SAT IT technician, who visits the site once a week.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board through the half termly school behaviour reports.

This list is not intended to be exhaustive.

3.4 The SAT ICT manager and technicians

The ICT manager and technician is responsible for ensuring:

- That the school's technical infrastructure is secure and not open to misuse or malicious attack.
- That the school meets required online safety technical requirements and any Local Authority or MAT online safety policies/guidance that may apply.
- That users may only access the networks and devices through a properly enforced password protection policy.
- That the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any one person.
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- That the use of networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the headteacher/DSL for investigation.
- That monitoring software/systems are implemented and updated as agreed in school policies.

This list is not intended to be exhaustive.

School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.

- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to school technical systems and devices.
- Internet access is filtered for all users.
- Internet filtering/monitoring should ensure that children are safe from terrorists and extremist material when accessing the internet.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices, etc. from accidental or malicious attempts which might threaten the security

of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up-to-date virus software.

3.5 Teaching and support staff

Are responsible for:

- Having an up-to-date awareness of online safety matters and of the current school online safety policy and practices.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2).
- Following the SAT email protocol and reminders (see appendix 6).
- Reporting any suspected misuse or online safety incident to the DSL or deputy DSLs via CPOMs or by filling in a pink form. The deputy head response for behaviour will then ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy (see appendix 5 for flowchart on dealing with unsuitable/inappropriate activities).
- Ensuring that all digital communications with pupils and their parents/carers should be on a professional level and carried out using official school systems.
- Teaching (support staff to support the teaching where appropriate) of the online safety strand of the computing curriculum and addressing online safety through other curriculum areas where relevant.
- Monitoring the use of digital technologies such as ipads, laptops etc in lessons and other school activities (where allowed) and implement current policies with regards to these devices.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Checking that websites intended to be used in lessons have been checked for suitability of use and ensuring that processes are in place for dealing with any unsuitable material that is found in internet searches including reporting this to the deputy DSL responsible for online safety.
- Alongside the SAT IT manager and technician, staff will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possibly and to report any concerns about the safety and security of school technical systems to the SAT IT team.

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 and understood the terms on acceptable use of the school's ICT 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

They can also visit the parents/carers area of the website esafetytraining.org, which acts as an excellent signpost to website links on various aspects of online safety.

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT 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 3).

4. Educating pupils about online safety

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

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

Online safety is a strand within our computing curriculum. Ensuring coverage of the four categories of risk (content, contact, conduct and commerce) this strand has been divided into eight areas informed by the Education for a Connected World framework. These areas are self image and identity; online relationships; online reputation; online bullying; managing online information; health, wellbeing and lifestyle and privacy and security. Our computing progression sets out the skills and knowledge related to these areas, which are taught in each year group – skills and knowledge build progressively each year. Knowledge and skills around online safety are also taught and/or revisited in other computing units, where relevant. Every two years online safety workshops are delivered to our children by 'the two Johns' from EST Online safety.

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

Pupils will be encouraged to discuss their concerns with their parents/carers as well as school staff. Many parents and carers have only a limited understanding of online safety risks and issues yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful

and inappropriate material on the internet and may be unsure about how to respond. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters and the school website.
- Parents evenings.
- High profile events such as Safer Internet Day.
- Biannual workshops run by two ex-police officers from EST E-safety to educate them on supporting their children to stay safe online at home and to raise awareness of current issues around online safety.
- Writing to all parents in a year group (and possibly wider) if there has been an online safety incident outside of school to raise awareness.
- DSL/deputy DSLs to support parents and signpost them to relevant information on an individual basis following an online safety incident (in or out of school)

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with 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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying 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. Each year group will teach a specific lesson on online bullying each year as part of the online safety strand.

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.

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

The headteacher, and any member of staff authorised to do so by the headteacher (as set out in our behaviour policy), 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 or deputy headteachers.
- 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.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the headteacher or authorised staff member to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent refuses to delete the material themselves

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

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
- Section 7.6 (confiscation, searches, screening) of 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.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers (if applicable) and governors ware expected to read and adhere to an agreement regarding the acceptable use of the school's ICT systems and the internet (appendix 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.

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

Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet. All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the school's online safety curriculum.

8. Pupils using mobile devices in school

Parents of children of child are able to complete a form giving permission for children in year 5 and 6 to bring their mobile phones onto the school site based on the following conditions:

- Children who bring their phones into school will need to take full responsibility for them.
- Phones must be switched off and kept in their school bag. They are not to be used at any time within the school day.
- The school take no liability or responsibility for children's phones and they are not covered by the school's insurance.
- Staff will not spend time searching for lost phones.
- Any child found to be using their phone at anytime within the school day will have their phone confiscated and may be told not to bring it back into school again.
- Any phone that rings during the school day will also be confiscated.
- If a child's phone is confiscated, the parent will be contacted and the phone will have to be collected from the school office by the parent, not the child.
- Children in year 5 and 6 must not bring other mobile devices (iPads etc) into school.

9. Staff using work devices outside school

All staff members and the SAT IT department, will take appropriate steps to ensure staff 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).
- Ensuring their hard drive is 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.
- Making sure the device locks if left inactive for a period of time.
- Not sharing the device among family or friends.
- Installing anti-virus and anti-spyware software.
- Keeping operating systems up to date by always installing the latest updates.

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 3.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice by emailing SAT IT support.

10. Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g., on social networking sites.
- Written permission from parents will be obtained when pupils join the school before photos of pupils are published on the school website/social media/local press.
- In accordance with guidance from the Information Commissioner's Office, parents are permitted to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites.
- Staff are allowed to take digital/images to support educational aims but these images should only be taken on school equipment.
- The personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, school twitter account or newspapers will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.

11. Social media

School staff should ensure that:

- No reference should be made to social media to pupils, parents/carers or school staff.
- They do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions are not attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise the risk of loss of personal information.

12. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our behaviour policy. 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 ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. 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.

It is hoped all members of the school community will be responsible users of digital technologies, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary, can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed and signed (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority
    - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of ‘grooming’ behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material o promotion of terrorism or extremism
    - offences under the Computer Misuse Act (see User Actions chart above)
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

13. Training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements (see appendix 3).
- The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, through attendance at external training events and by reviewing guidance documents released by relevant organisations and at least annually.

- This online safety policy and its updates will be shared with staff.
- Refresher training will be delivered at least once each academic year to staff members as part of safeguarding training, as well as relevant updates as required (for example through emails, weekly briefing notes and staff meetings).
- All teaching staff will receive external online safety training, currently from ‘esafety training - The 2Johns’ at least every two years.
- The DSL or deputy DSLs will provide advice/guidance/training to individuals as required.

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

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. They are also invited to take part in the biannual training from ‘esafety training – The 2Johns’.

Volunteers will receive appropriate training and updates, if applicable.

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

14. Monitoring arrangements

The deputy headteacher, responsible for behaviour, logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 4.

This policy will be reviewed every two years by the computing subject leader. At every review, the policy will be shared with the governing board. The review will be informed by any updated guidance and will consider and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS

When I use the school's ICT systems (like computers and ipads) and get onto the internet in school I will:

- Ask a teacher or adult before using a computer or ipad
- Only use websites or apps that a teacher or adult has told me or allowed me to use
- Tell my teacher immediately if:
    - I click on a website by mistake
    - I receive messages on an ipad or computer from people I don't know
    - I find anything that may upset or harm me or my friends like a horrible image or nasty words
- Use school computers and ipads for school work only
- Make sure that what I type or paint on a computer is appropriate and kind
- Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
- Only use the username and password I have been given
- Try my hardest to remember my username and password
- Never share my password with anyone, including my friends
- Never give my personal information (my name, address or telephone numbers) to anyone unless my teacher or parent says that I can
- Check with my teacher before I print anything
- Close the apps or programs that I have been using when I have finished
- Log off or shut down a computer when I have finished using it

I understand that the school will check the websites I visit and that if I must follow the rules above.

Appendix 2: KS2 acceptable use agreement (pupils)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material which is inappropriate or offensive and might upset, distress or harm me or others
- Always shut close the programs or apps I have been using and to then log off or shut down a computer or device when I've finished working on it

I will not:

- Access any inappropriate websites, including social networking sites, chat rooms and gaming sites unless my teacher has allowed this as part of a learning activity
- Click on any pop-ups or messages on websites that I am not sure about
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is inappropriate or offensive and might upset, distress or harm me or others
- Log in to the school's network using someone else's details
- Bring personal electronic devices like mobile phones or tablets into school unless I have permission (Year 5 and 6 only).
- If I do have permission to bring a mobile phone into school (Year 5 and 6) I understand that it must be switched off at all times whilst on the school site.

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school
• I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. • I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy. • I will let the designated safeguarding lead (DSL) or deputy designated safeguarding leads know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. • I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Appendix 4: Format of form for recording online safety incidents

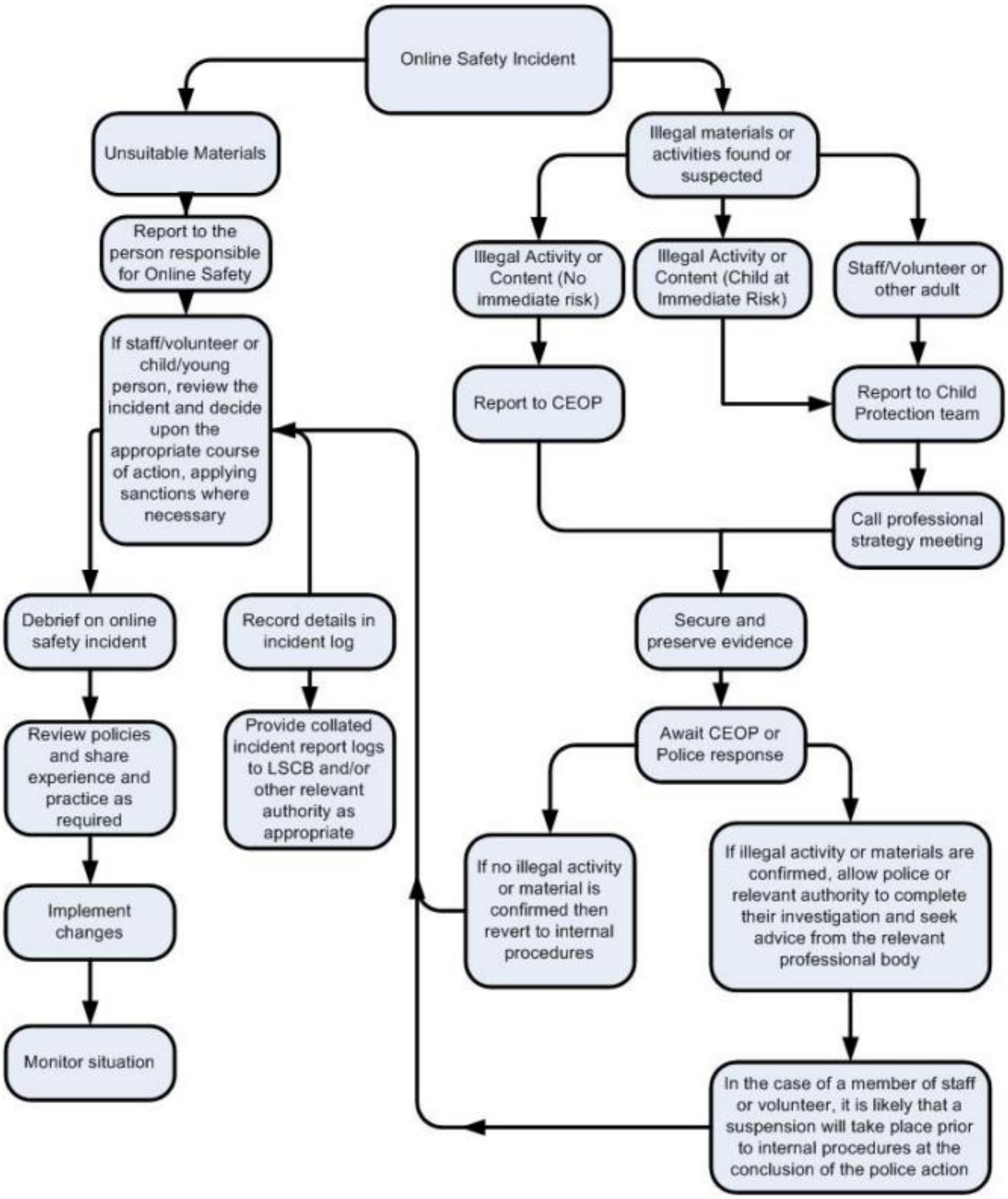
Records of poor behaviour are recorded on the 'infant/junior behaviour log'. Further details, if the incident is deemed serious or a safeguarding issue, are recorded on CPOMs.

This document provides records and analysis of the following:

- Exclusions and suspensions
- Use of internal isolation
- Bullying
- Discriminatory and prejudiced behaviour, either directly or indirectly, including racist, sexist, disability and homophobic/biphobic/transphobic bullying
- Use of derogatory language
- Sexual harassment and/or sexual violence
- Restrictive physical intervention
- Online safety incident

Date of incident	Type of incident	Details of children	Details of incident	Action Taken (including date)

Appendix 5: Dealing with unsuitable/inappropriate activities



Appendix 6: SAT email protocols and reminders

These are issued to staff when they commence employment at Katherine Semar Schools.

Before sending emails consider:

- The maintenance of the highest professional standards.
- Whether email is the correct medium for communication.
- The expected communication style – communication with parents should keep a formal/professional style at all times.
- Only copy in people who have an immediate need for the information.
- The length of the email- avoid long detailed emails.
- Time required for the recipient to respond. We would like to REDUCE email traffic in our schools as this impacts on staff workload. Consider giving messages out at staff briefings, staff meetings or face to face

Remember:

- **You MUST NOT** give anyone's email address out without their consent – this includes when you email a group of parents – you must use Bcc (Blind Carbon Copy)to ensure you are not unintentionally sharing email addresses. Click on "options" to find this when writing an email.
- Under *no* circumstances should staff contact students, parents or conduct any school business using any *personal* email addresses.
- Never email in haste, consider the facts and consequences of the message.
  Be professional and careful about what you say about others, as email is easily forwarded. Only put in writing what you would say to someone's face. When needing to vent frustration about a workplace situation, particularly if you are angry, wait to calm down so your response is more measured.
- If any issues /complaints are involved then staff sending emails to parents, external organisations, or students are advised to cc their line manager/s and other relevant individuals.
- Never use email for:
  - performance appraisal or review, always do it face-to-face.
  - Human Resource issues (salary, job, career progression).
  - complex issues as these should be discussed at meetings.
- Staff are responsible for the security of their computer, and for protecting any information or data used and/or stored on it. Do not to leave a mailbox open and unattended, always keep it password protected. The account holder/s must keep their passwords confidential to prevent other users from accessing and sending emails from their account.
- Do not send whole school emails unless essential for school business
- Do not send or forward attachments unnecessarily.
- Emails may be monitored and absent staff should be aware that their email account may be opened by a senior member of staff/admin team if required (see SAT Code of Conduct)
- Never use your work email address when posting comments on public bulletin boards or chat rooms unless directly related to your work.
- If you receive an email that is obviously spam or of an adult nature, do not open it, rather delete it immediately.
- Never participate in chain emails where you are asked to forward an email to a number of others.
- In legal terms, under the Telecommunications Regulations 2000, sending an email is as binding as sending a signed letter. Therefore, do not express personal views or information by email, because as an employer, SAT could be held vicariously liable for the opinions and views expressed. This also applies to comments posted on public discussion boards if you use the school email address or state the opinions in a work capacity. Never send emails that are offensive, threatening, defamatory or illegal. Emails have been used successfully as evidence in libel cases. Be aware of copyright and libel issues e.g. when sending scanned text, pictures or information downloaded from the internet.
- Be aware that emails created or received as part of your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Always read and reflect upon your email before sending

Sensitive Information in Emails

Sensitive personal information includes any health, residential, contact or SEND information.

- Emails are the electronic equivalent of a postcard. Anyone can read the content along the delivery path. Sensitive information should usually be sent by post or via a secure transfer system. Where the conclusion is that your school email must be used to transmit such data, then exercise caution when sending the email and *always* follow these checks *before* releasing the email:
    - Verify the details, including accurate email address, of any intended recipient of the information.
    - Do not copy or forward the email to any more recipients than is absolutely necessary.
    - Do not send the information to any person whose details you have been unable to separately verify.
    - When sending an email containing personal or sensitive data, the name of the individual is not to be included in the subject line
    - To provide additional security you need to put 'CONFIDENTIAL' in the subject line and as a header in the email and any attachments to the email.
- Any email containing sensitive personal information (about staff or students) being sent by you to a recipient who **does not have an KS email address** MUST be encrypted or sent with password protection. Ask ICT support if you need help with this.
- Child Protection issues MUST NOT be reported via email. You must hand in the forms directly to designated staff