Somerleyton Primary School

Online Safety Policy

Signed ……

Author: Governing Body

Publish Date: September 2025

Review Date: September 2026

SOMERLEYTON SCHOOL Policies

Contents

1. Introduction
2. Aims
3. Policy development, monitoring and review
4. Legislation
5. Process for monitoring the impact of the Online Safety Policy
6. Roles and Responsibilities
7. Teaching and learning
8. Risks
9. Reporting

Introduction

This Online Safety Policy outlines the commitment of Somerleyton Primary School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Somerleyton Primary School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

Aims

This policy aims to explain how staff, parents/carers, children or young people can be a part of these safeguarding procedures. It also details how children are educated to be safe and responsible users capable of making good judgements about what they see, find and use. The term 'Online Safety' is used to encompass the safe use of all technologies in order to protect children and adults from potential and known risks. This policy establishes clear mechanisms to identify, intervene and escalate an incident, where appropriate. We aim to:

- To emphasise the need to educate staff and children about the pros and cons of using new technologies both within and outside of Somerleyton Primary School.
- To provide safeguards and agreement for acceptable use to guide all users, whether staff and children in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the boundaries of our school.
- To develop links with parents/carers and the wider community to enable the school to share both an awareness of the benefits and potential issues related to technologies.

Policy development, monitoring and review

This Online Safety Policy has been developed through consultation between:

· headteacher

· Designated safeguarding lead (DSL)

· Online Safety Lead (OSL)

· staff – including teachers/support staff/technical staff

· governors

· parents and carers

Legislation

This policy is based on the Department for Education's (DfE) 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
- 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.
This policy complies with our funding agreement and articles of association.

Process for monitoring the impact of the Online Safety Policy

The school will monitor the impact of the policy using:

- logs of reported incidents
- Filtering and monitoring logs
- internal monitoring data for network activity
- surveys/questionnaires of:
    - Learners
    - parents and carers
    - staff.

Roles and Responsibilities

- The Online Safety Lead is: Oliver Clifford
- The School's Senior Designated Professionals for Safeguarding are: Oliver Clifford and Victoria Speed Andrews.

The responsibility of managing Online Safety can be demanding and challenging and therefore all staff must take responsibility and ownership.

It is the duty of parents/carers to ensure that their child/children remain safe outside of school when using the internet and other electrical devices. While every possible measure is taken within school and term time, to ensure children and adults are safe, if parents/carers have concerns about material and content on the schools website they should report it to the Online Safety Leader as soon as possible or as soon after a school holiday as at all possible.

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 include regular opportunities with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All Governors will:

- Ensure they have read and understood this policy
- Agree and adhere to the terms on acceptable use of school's ICT systems and the internet (See Acceptable Use Policy)
- Receive reports of online safety incidents
- Check the provision outlined in the Online Safety Policy is taking place as intended
- Ensure that filtering and monitoring provision is review and recorded at least annually
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND 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

2. The Headteacher

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher and (at least) another member of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff
- The headteacher is responsible for ensuring that the Designated Safeguarding Lead / Online Safety Lead, IT provider/technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- The headteacher/senior leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- The headteacher will receive regular monitoring reports from the Designated Safeguarding Lead / Online Safety Lead.
- The headteacher will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.

3. The Designated Safeguarding Lead

Details of the school's DSL are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

The DSL 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 ICT manager, Online Safety Lead 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, including understanding the filtering and monitoring systems and processes
- 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 4 contains a 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 governing board

This list is not intended to be exhaustive.

4. The ICT Manager

The ICT manager is 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 ICT 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 ICT systems on a regular basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

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 ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- 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'
- Undertake the appropriate training which amongst other things includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring
- Reading newsletters and updates which pertain to aspects of online safety and safeguarding

This list is not intended to be exhaustive.

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 ICT systems and internet

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
- Healthy relationships – Disrespect Nobody

- National College – National Online Safety | News | National Online Safety (nationalcollege.com)
- Online Safety Newsletter - Somerleyton Primary School - Online Safety - Parents

7. Visitors to school

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

Teaching and learning

- The purpose of Internet use is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- The Internet is an essential element for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Curriculum

Pupils will be taught about online safety as part of the curriculum, and through bespoke online safety workshops using Purple Mash's '2 Be Safe in a Digital World' scheme, which in turn is aligned with the DfE's Education in a Connected World.

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

We will 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)

Online Safety Leaders

Year 6 representatives take on the role of Online Safety Leaders. They champion online safety across the school and its wider community. They have special responsibility for promoting online safety throughout the school. These online safety champions could be involved with:

- Reporting to the School council and offering advice.
- Organising online safety posters for the classrooms
- Checking the school website for parent-friendly and child-friendly online safety
- information.
- Organising and presenting an online safety assembly
- Thinking of ideas for activities for Safer Internet day
- Drafting age-appropriate Access User Agreements

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between pupils world-wide through the video-conferencing;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with DfES;
- access to learning wherever and whenever convenient.

The Internet enhancing learning

- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

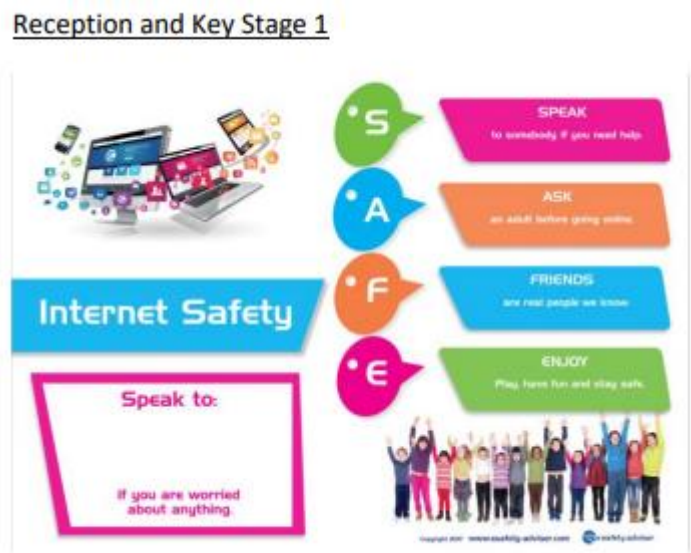
Educating Parents about Online Learning

The school will raise parents' awareness of internet safety in letters, newsletters, online safety cafes and in information via our website This policy will also be shared with parents. Online safety will also be covered during parents' evenings.

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

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

Online Safety Responsibilities:



Key Stage 2

Risks

There are many potential risks for children and young people including:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, 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 scam

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. Class teaches will discuss Cyber Bullying with their class as well as liaising with our local PCSO for expert advice.

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.

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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

WHAT ELSE MIGHT BE OF CONCERN?

A child who:

- Is becoming secretive about where they are going to or who they are meeting.
- Will not let you see what they are accessing online.
- Using a webcam in a closed area, away from other people.
- Accessing the web or using a mobile or PDA (Personal Data Assistant) for long periods and at all hours.
- Clears the computer history every time they use it.
- Receives unexpected money or gifts from people you don't know.

An adult who:

- Befriends a child/children or young person/people on the internet or by text messaging.
- Has links to children or young people on their Facebook or other social network site; (see AU ICT Policy).
- Is secretive about what they are doing and who they are meeting.

MITIGATING RISKS

- Keep the computer/s in a general space where we can monitor what is going on.
- Explain the risks of giving out personal details online.
- Talk about how people can be anyone they want to be online (Catfishing): by using misleading emails, photographs of other people, telling lies about their age, school, hobbies.
- Encourage children and young people to think carefully about which photographs or videos they use on line this material can be used and tampered with by other people, or they may not be appropriate.
- Advise children to only text, chat or webcam to people they know for real and under the guidance of family or school i.e. skype to other schools as a group.

- Advise children to only play online games with people they know and to let their parents know beforehand.
- Discuss how people hide their identities online and the importance of never meeting new online “friends” for real.
- Make sure children and young people understand they can talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
- Look on the internet together for information about how to deal with, or report, problems.
- Talk about how, when information or images get onto the net, they can never be erased or retrieved.
- Training/information for staff and parents on E-safety - updated annually.
- Ensure that images, photographs and video taken for educational purposes are deleted once used.
- Children are not allowed to bring in internet-enabled devices or recording features.
- Governor monitoring that ensures pupils and staff understand the procedures of the school. Governor monitoring will ensure that pupils are receiving education in Online Safety.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the Headteacher to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.

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

- The DfE’s latest guidance on screening, searching and confiscation

- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The school's COVID-19 risk assessment

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

Evaluating Internet content.

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider via the Head teacher.
- Pupils will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.
- The evaluation of on-line materials is a part of every subject.

Managing Internet Access

- The security of the school ICT systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The IT technician will review system capacity regularly.

Filtering and Monitoring

Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filtering and monitoring systems in place and regularly review their effectiveness. They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified. Governing bodies and proprietors should consider the number of and age range of their children, those who are potentially at greater risk of harm and how often they access the IT system along with the proportionality of costs versus safeguarding risks.

The appropriateness of any filtering and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

• identify and assign roles and responsibilities to manage filtering and monitoring systems

• review filtering and monitoring provision at least annually

• block harmful and inappropriate content without unreasonably impacting teaching and learning

• have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard.

Published Content - Website

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The head teacher or named governor, will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The Web site should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Photographs that include pupils will be selected carefully and written consent will be sort by parents/carers when children start school.
- Pupils' full names will not be used anywhere on the Web site, particularly in association with photographs.

Social networking and personal publishing

- Filtering carried out through Smoothwall.
- Proxy settings and anti-virus regularly checked by ICT technician
- Proxy level higher for pupil access than teacher
- Pupils are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils are advised not to place personal photos on any social network space. They consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name, school, shopping centre.
- Somerleyton Primary School is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.
- The school will work in partnership with parents; the CSA, DfES and the Internet Service Provider to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported to the Internet Service Provider.
- Any material that the school believes is illegal must be referred to the Internet Watch Foundation
- The School's social media is accessible only by the Headteacher and Administration Assistant. They take responsibility to anything that is uploaded.

Emerging technologies and wearable devices

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and other internet-enabled devices will not be used in areas of the school populated by pupils. The sending of abusive or inappropriate text messages is forbidden.

Risk Assessment

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.
- Methods to identify, assess and minimise risks will be reviewed regularly.
- The head teacher will ensure that the Online Safety Policy is implemented and compliance with the policy monitored.

Online Safety complaints

- Complaints of Internet misuse will be dealt with by the head teacher or Chair of Governors.
- Any complaint about staff misuse must be referred to the head teacher.

Internet used across the community

- The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites and internet linked games and offer appropriate advice.

Communications

- Rules for Internet access will be shared with pupils by teachers.
- Rules and advice for children visible in every class.
- Pupils will be informed that Internet use will be monitored.
- A module on responsible Internet use will be included in the PSHE programmes covering both school and home use.

Employees

- All staff must accept the terms of the 'Responsible Internet Use' statement before using any Internet resource in school.
- All staff will be given the Somerleyton Primary School e-Safety Policy and its importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff development in safe and responsible Internet use and on the school Online Safety Policy will be provided as required.
- Staff will not use personal devices to take pictures whilst on trips.

Reporting

The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- there are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- all members of the school community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received the Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.

WHAT DO I DO IF I AM CONCERNED?

If you have any concerns speak to the Online Safety Lead or a Designated Safeguarding Lead immediately.

CONTACTS FOR REFERRING

If the concern is about:

- A child being in imminent danger, ALWAYS DIAL 999 FOR THE POLICE.
- The welfare of a child, discuss your concerns immediately with the Senior Designated Person for Safeguarding, Oliver Clifford, or the alternate professional, Victoria Speed Andrews
- Ring the local children's social care services- Customer First: 0808 800 4005 or access what to do by going to www.suffolkscb.org.uk
- A known person's sexual behaviour or intentions ring the local children's social care services.
- A person who has a "duty of care" within the organisation, immediately speak with the Head teacher or Chair of Governors.
- An unknown person's sexual behaviour or intentions, report at www.ceop.gov.uk (Child Exploitation and Online Protection Centre).
- Harmful content, including child sexual abuse images or incitement to racial hatred content contact www.iwf.org.uk

REMEMBER IT IS YOUR RESPONSIBILITY TO ENSURE THAT YOU:

- **DO NOT DELAY.**
- **DO NOT INVESTIGATE.**

- **ISOLATE ANY EQUIPMENT AND PREVENT FURTHER USE OF AN ONLINE ACCOUNT.**
- **MAKE CAREFUL RECORDING OF ANYTHING YOU OBSERVE OR ARE TOLD.**
- **SEEK ADVICE FROM THE LEAD OR DEPUTY PERSON FOR E-SAFETY.**
- **REFER IMMEDIATELY.**
- **MINIMISE THE RISKS:**

Links with other policies

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy
- Complaints procedure
- ICT and internet acceptable use policy

APPENDIX A

Somerleyton Online Safety Recording Form

Please refer to the Online Safety Policy

Name of student/person	Date	Tutor Group/ Form/Class	**Your name** (and position in school)

Nature of Internet Concern

……..

……

……..

……..

……

……

Has this happened before?	Yes		No					
Did you report the previous incident?	Yes		No		To Whom?		Date:	

*If yes, discuss this with your e-Safety Lead, follow the e-safety reporting flow chart and ensure that this is recorded on the e-Safety Lead's log.

This recording form is for e-safety concerns/breaches.

As well as recording these on this form you should add to the e-safety log (in office) and refer to the appropriate person:

- Head teacher
- Police—See E-Safety policy for guidance but would include

⇒ deliberately accessing or trying to access material that is considered illegal such as offensive or pornographic material

APPENDIX B

Acceptable Use Policy Reception and Key Stage 1

Somerleyton Primary School

All pupils in the Early Years and Key Stage 1 must follow the rules in this policy when using school computers and ICT equipment. We understand that the rule s in the policy will help to keep us safe and happy.
Pupils that do not follow these rules may find:

- They are not allowed to use the computers,
- They can only use the computers if they are more closely watched.

Pupil Acceptable Use Policy Early Years and Key Stage 1	
1	I only use the internet when an adult is with me
2	I keep my personal information and passwords safe
3	I only send messages online which are polite and friendly
4	I know that staff at Somerleyton Primary School can see what I am doing when I use Somerleyton laptops and tablets, and when using Purple Mash at home.
5	I always tell a trusted adult if something online makes me feel upset, unhappy or worried.
6	I know that if I do not follow the rules, I may not be able to use certain technologies or websites to help me learn
7	I have read and talk about these rules with my parents/carers.

UNACCEPTABLE USE

Examples of unacceptable use include, but are not limited to:

Using a computer with another person's username and password.
Creating or sending on the Internet any messages that might upset other people.
Looking at, or changing work that belongs to other people.

APPENDIX C

Acceptable Use Policy Key Stage 2

All pupils in Key Stage 2 must follow the rules in this policy when using school computers and ICT equipment. We understand that the rule s in the policy will help to keep us safe and happy. Pupils that do not follow these rules may find:

- They are not allowed to use the computers,
- They can only use the computers if they are more closely watched.

	Pupil Acceptable Use Policy Key Stage 2
1	I will only use polite language when using the computers.
2	I must not write anything that might: upset someone or give the school a bad name.
3	I know that teachers will regularly check what I have done on the school computers.
4	I know that if a teacher thinks I may have been breaking the rules they will check on how I have used the computers before.
5	I must not tell anyone my name, where I live, or my telephone number - over the Internet.
6	I must not tell my username and passwords to anyone else but my parents.
7	I must never use other people's usernames and passwords or computers left logged in by them.
8	If I think someone has learned my password then I will tell my teacher.
9	I must log off after I have finished with my computer.
10	I must not use the computers in any way that stops other people using them.
11	I will report any websites that make me feel uncomfortable to a member of staff.
12	I will not try to harm any equipment or the work of another person on a computer.

APPENDIX D

Acceptable Use Policy Staff

Appendix 1 **Acceptable Use Rules for Staff**

To ensure that all adults within the school setting are aware of their responsibilities when using any on-line technologies, such as the Internet or E-mail, they are asked to sign and follow these rules.

I have read and understand my responsibilities within the Acceptable Use policy.

I know that I should only use the school equipment, software and online resources (including email) in an appropriate manner and for professional uses.

I have read the procedures for Incidents of Misuse so that I can deal with any problems that may arise, effectively.

I will report accidental misuse.

I will report any incidents of concern for children's safety to the head teacher, designated person for Safeguarding.

I know who my Designated Person for Safeguarding is

I know that I am putting myself at risk of misinterpretation and allegation should I contact children and young people via personal technologies, including my personal e-mail and should only use the school email and phones.

I know that I should not be using the school system for personal use unless this has been agreed by the Head teacher.

I know that I should follow the advice given about the use of Social Networking sites in order to protect myself given the public nature of these sites.

I know that I must not use gaming platforms during school hours.

I know that I should ensure my anti-virus is updated on my laptop so that I do not inadvertently transfer viruses, especially where I have downloaded resources.

I will only install hardware and software I have been given permission for.

I will ensure that I follow the Data Protection Act 2018 for data protection laws in the UK and have checked I know what this involves.

I will ensure that I keep my password secure and not disclose any security information unless to appropriate personnel. If I feel someone inappropriate requests my password, I will check with the Head teacher.

I will adhere to copyright and intellectual property rights.

I will not upload personal media files or other personal files onto the school network.

I understand that I will return any school equipment when I leave the school.

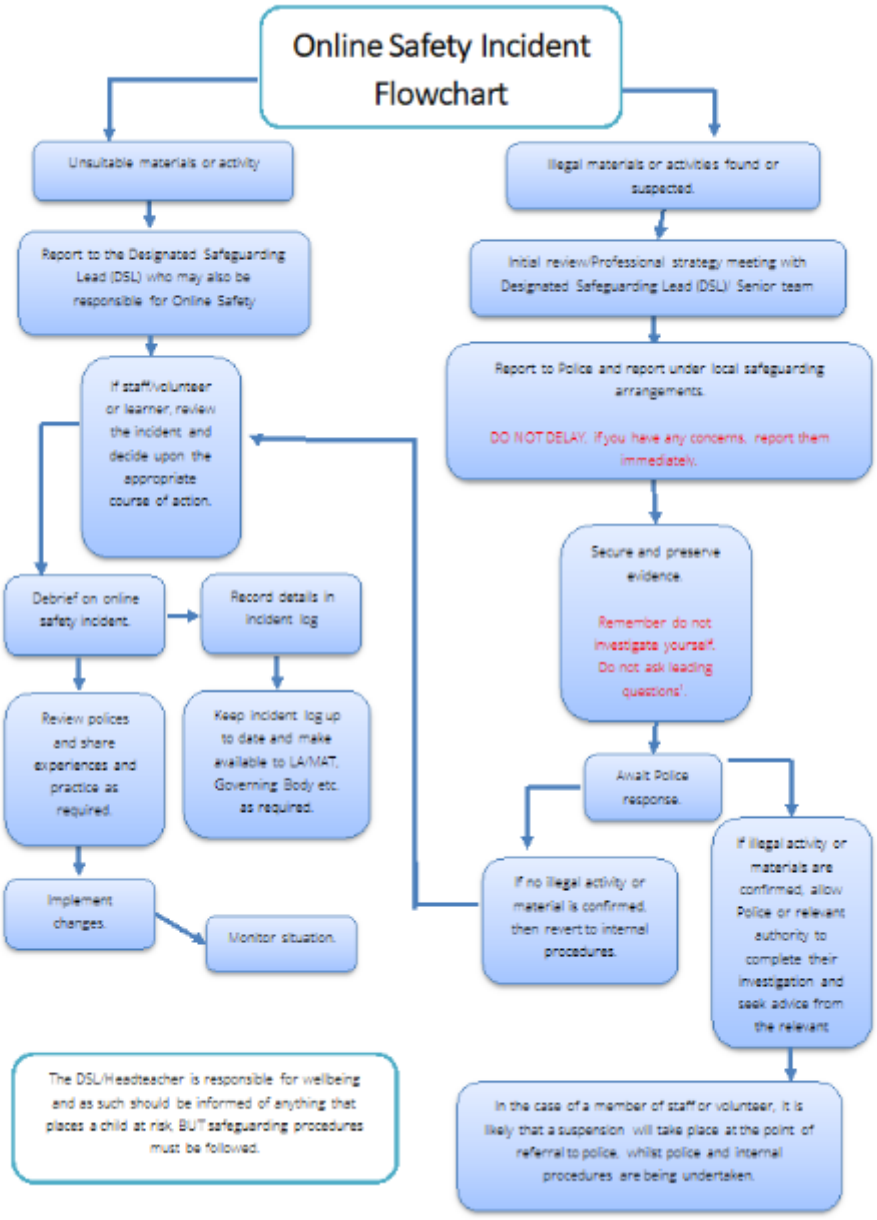
I will ensure that during school time any wearable devices I have, as with mobile phones, are on 'silent mode' and stored away from children and used only in the staff room discretely.

I will ensure that during school time my mobile phone is in 'silent mode' and stored and used discretely.

I have read, understood and agree with these Rules.
Signed……Date…….

Name ……

APPENDIX E


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL) Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY. If you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions!.
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.