Sutton Veny CofE Primary School
Online Safety Policy

Together, through **friendship**, in **peace** and with **courage**, we reach for the stars.

Colossians 3:12: '**clothe yourselves** with **compassion**, **kindness**, **humility**, **gentleness** and **patience**.'

Our Aims:

Our school aims to:

- Have robust processes in place to ensure the online safety of all 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.
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Why internet and digital communications are important:

- The purpose of technology in schools is to raise educational standards, to promote achievement, to support the professional work of staff and to enhance the school's management functions.
- Sutton Veny CofE Primary School strives to provide pupils with quality internet access as part of their learning experience.
- Internet use is part of the statutory curriculum and a necessary tool for staff.

The four key categories of risk:

It is essential that children are safe from potentially harmful and inappropriate online material. An effective whole school approach on online safety empowers us to protect and educate pupils and staff in their use of technology and establishes mechanisms to identify, intervene in and escalate any concerns where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

content: *being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.*

contact: *being subjected to harmful online interaction with other users; for example: 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: *online behaviour that increases the likelihood of, or causes, harm; for example, 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.*

Roles and Responsibilities:

It is the responsibility of all adults and pupils linked to Sutton Veny CofE Primary School to ensure that this policy is implemented fully.

The governing board:

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

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 1).
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school approach to safeguarding and related policies and/or procedures.
- Ensure that filtering and monitoring provision is reviewed 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 special educational needs and/or disabilities (SEND).

The head teacher and Senior Leaders:

The head teacher and Senior Leaders are responsible for:

- Establishing and reviewing the school online safety policies and documents, and presenting any updates for discussion with staff.
- Ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

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.

The DSL takes responsibility for online safety in school and, as such, is also the Online Safety Lead. The DSL will:

- Put 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.
- Ensure that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Regularly monitor the school's ICT systems.
- Block access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

- Ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensure that any incidents of cyber-bullying are dealt with appropriately in line with the school's behaviour policy.
- Liaise with the school technician to ensure that the technical infrastructure is secure, the school meets required online safety technical requirements, including filtering and virus protection, and that the appropriate access is provided for users.
- Support staff to understand this policy and to ensure that it is being implemented consistently throughout the school.
- Work with the Computing lead and other staff, as necessary, to address any online safety issues or incidents relevant to improving the curriculum.
- Coordinate staff training on online safety.
- Liaise with other agencies and/or external services if necessary.
- Provide regular reports on online safety in school to the governing board.

The Computing Lead:

The Computing Lead is responsible for:

- attending relevant meetings with the Online Safety Governor to discuss current issues.
- meeting with Digital Leaders to discuss their responsibilities related to online safety (Appendix 2) and to share the pupils' views on online safety.
- ensuring pupils are involved in the development of e-safety rules.
- planning a differentiated online safety curriculum, appropriate to each age group.
- ensure that the online safety element of the curriculum is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND).
- organising an annual E-Safety week to further enrich and strengthen the children's e-safety learning.
- ensuring that key online safety messages are reinforced through relevant assemblies.
- receiving regular updates through attendance at external training events and by reviewing guidance documents.
- keeping up-to-date with developments in how AI (artificial intelligence) can support classroom learning and sharing this, and the ways to mitigate the associated online safety risks, with staff and governors.
- supporting pupils to understand how generative AI works, its potential benefits, risks, and ethical and social impacts and equipping learners with the knowledge, skills and strategies to engage responsibly with AI tools.

The PSHE Lead:

The PSHE Lead is responsible for:

- Developing and monitoring Digital Wellbeing units as a part of the PSHE curriculum.

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 the Online Safety: Personal Use of Social Media Policy (Appendix 3), 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'.
- Promoting e-safety regularly with pupils, ensuring online safety is embedded in all aspects of the curriculum and other activities.

Parents and Carers:

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The school takes every opportunity to help parents/carers understand these issues through newsletters, courses, the website and national online safety campaigns. Parents and carers are encouraged to support the school in promoting good online safety practice by:

- keeping digital and video images taken at school events private, and not sharing them on wider social media platforms.
- providing written consent before photographs of pupils are published on the school website or in the local press.
- signing the pupil's Acceptable Use Agreement that they sign annually in their Link Books (Appendix 4a and 4b).
- Notifying a member of staff or the head teacher of any concerns or queries regarding this policy.

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 5). Guests such as trainee teachers, supply teachers and visitors will be provided with temporary passwords to access the school systems.

Pupils:

The education of pupils in online safety and digital literacy is an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience. Pupils:

- are responsible for using the school digital technology systems in accordance with the pupil's Acceptable Use Agreement that they sign annually in their Link Books (Appendix 4a and 4b).
- are taught to tell an adult if anything is worrying them online, including texts and emails, and they are taught how to report abuse or misuse at KS2.
- learn about the importance of adopting good online safety practice when using digital technologies out of school and explore how the school's online safety policy covers their actions out of school.
- access the server through class (FS2 – Year 4) or individual (Year 5 – Year 6) passwords.

- must not take images of others without their permission.
- use a whole class email address when sending emails, writing their messages in a polite and friendly manner.

IT Provider:

The school's ICT system is reviewed regularly and our virus protection is regularly updated by the school's computing technician (external provider).

The IT service provider has technical responsibility for:

- maintaining filtering and regularly monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

The IT service provider works closely with the head teacher/DSL to:

- procure systems
- identify risk
- carry out reviews

The computing technician will follow and implement the school's Online Safety Policy and procedures. Ultimately, it remains the responsibility of the head teacher to ensure that the school's computing technician carries out all the online safety measures that the school's obligations and responsibilities require.

Filtering and Monitoring:

- To safeguard and promote the welfare of children at our school and to provide them with a safe environment in which to learn, we limit children's exposure through appropriate filtering and monitoring on school devices and school networks.
- Regular reviews take place to identify their effectiveness.
- 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.
- Parental communications to reinforce the importance of children being safe online is provided to understand of what systems the school use to filter and monitor online use. The importance for parents and carers to be aware of what their children are being asked to do online, is taken in to account, including the sites they will be asked to access and who their child will be interacting with online.
- Online safety is informed in part, by the risk assessment required by the school's statutory Prevent Duty.

Emailing:

- Staff may only use approved email accounts on the school system.
- All in-coming emails should be treated as suspicious and attachments should not be opened unless the author is known.

- The forwarding of chain letters is not permitted.

Cyber Security:

- Staff and governors receive training on the common cyber security threats and incidents that schools experience.
- The school's curriculum offer includes cyber awareness for our learners.

Published Content and the School Website:

- The contact details on the school's website are the school address and phone number; no staff or pupil's personal details will be published.
- The head teacher has overall editorial responsibility of the website to ensure that content is accurate and appropriate.

Publishing pupils' images:

- Photographs that include identifiable images of children should only be added to the school's website with consent from the parent/carer.
- Where photos are added to the school's Facebook page, the back of the children is shown.
- Pupil's full names will not be cited on the website nor on the Facebook page.
- Parents are informed about our school policy on image taking and publishing.

Social Networking:

- The school does not allow use of any social network sites for children.
- The school uses a private and secure Facebook account.
- Where parents have organised a Facebook class page or Whatsapp group outside of school they are required to adhere to the school's Parental Code of Conduct.

Mobile Phones:

- Pupils are not permitted to bring mobile phones, nor smart watches, into school.
- The school recognises youth produced sexual imagery, sharing of nude and semi-nude images (previously known as "sexting") as a safeguarding issue; all concerns should be reported to and dealt with by the Designated Safeguarding Lead (DSL).

Video Conferencing:

- Video conferencing is always supervised.
- Any video conferencing will use the educational broadband network to ensure quality of service and security.

Managing Emerging technologies:

- The school will examine emerging technologies for their educational benefit and carry out a risk assessment before use in school.
- Mobile phones and associated cameras will not be used in lessons or school time as part of an educational activity, although school mobile phones are permitted to be used by staff for photos and school-related phone calls.
- Staff will not use personal mobile phones on site during the school day.

Network management:

- The school uses individual, audited log-ins for all staff users.
- Storage of all data within the school will conform to the UK data protection requirements and subsequent General Data Protection Regulation (GDPR).

Protecting Personal Data:

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Policy Decisions:

Authorising internet access:

- All staff, governors and visitors must read and sign the 'Acceptable Use/ICT Code of Conduct' before using any school ICT resource.

Assessing Risks:

- The school will take reasonable precautions to prevent access to inappropriate material; however, it is not possible to guarantee that unsuitable material will never appear on a school ICT resource.
- The school will monitor ICT use to establish if the e-safety policy is appropriate and effective.

Arrangements for reporting e-safety incidents inside school:

- If a child has been exposed to unsuitable, inappropriate or illegal material the flow chart in Appendix 6 must be followed.
- If available, any evidence must be kept.
- The head teacher must be informed as soon as possible, so that the best course of action can be decided upon – this may include school-based sanctions, meetings with parents and, in the most severe incidents, the police may be involved.
- All incidents must be recorded and logged.

Outside School:

- As soon as a member of staff is made aware of any e-safety incident, they must follow the guidance above.
- Parents should always be informed when e-safety incidents occur outside of school.
- Children are regularly reminded of how to keep safe online and if any incidents were to occur, what they must do. They are also made aware of CEOP www.ceop.police.uk and Childline www.childline.org.uk 0800 1111.

Handling e-safety complaints:

- Complaints of internet misuse will be dealt with by the head teacher.
- Complaints of misuse by staff will also be dealt with by the head teacher.
- Any complaints of a child protection nature will be dealt with in accordance to child protection procedures. The flow chart (Appendix 6) will be used where appropriate.
- Pupils and parents will be informed of the consequences and sanctions for pupils misusing the internet and this will be in line with our Behaviour Policy.

Communicating Our Policy:

Pupils:

- Appropriate sections of this policy will be shared with pupils.
- E-safety rules will be visible around school and pupils will be involved with the development of these.
- Age-appropriate curriculum opportunities will be used to ensure all pupils gain an awareness of e-safety. These will be addressed on a regular basis and modified as newer risks are identified.

Staff:

- All staff will be given a copy of the e-safety policy and will sign the acceptable use policy.
- Staff will be made aware that the system is monitored and that professional standards are expected.
- In line with KICSIE 2025, new staff have online checks carried out as part of our recruitment process.

Parents:

- Parents will be notified of the policy in newsletters and on the website.
- All parents/carers will be asked to sign the pupil/parent agreement when they register their children.
- Parents will be offered e-safety training (in-house or as part of the Compass Schools Collaboration) to encourage them to support and encourage positive online activities with their children and help them to use the internet safely.

National Links and Resources for Parents/Carers:

- Action Fraud: www.actionfraud.police.uk
- CEOP: www.thinkuknow.co.uk www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Lucy Faithfull Foundation: www.lucyfaithfull.org
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk

This policy is to be read in conjunction with the school's Safeguarding and Child Protection Policy, including the Behaviour Policy and Anti Bullying Policy, as well as the Staff Code Of Conduct.

Approved by:	Full Governing Body	**Date:** April 2026
Last reviewed on:	April 2026	
Next review due by:	April 2027	

Appendix 1:

Online Safety: Acceptable Use Policy Agreement for Governors and Friends of School

1. I will use the email account issued to me in an appropriate way. I will not:
   - access offensive emails or download offensive material
   - make personal use of the e-mail account
   - copy information from the Internet that is copyright or without the owner's permission
   - send e-mails that are offensive or otherwise inappropriate
   - disregard my responsibilities for security and confidentiality
   - access the files of others or attempt to alter the email account settings.
2. I will only access the account with my own name and registered password, which I will keep secret.
3. I will inform the Head Teacher as soon as possible if I know my password is no longer secret.
4. I will always log off the system when I have finished working. ·
5. I understand that the school may, in line with policy, monitor and check my e-mails.
6. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.
7. I will not open e-mail attachments unless they come from a recognised and reputable source. I will bring any other attachments to the attention of the Head Teacher.
8. All joke e-mails and attachments are potentially damaging and undesirable and therefore must not be used.
9. I will report immediately to the Head Teacher any unpleasant material or messages sent to me.
10. Activity that threatens the integrity of the school is forbidden.
11. I understand that if I do not adhere to these rules my email account will be suspended immediately and that other disciplinary consequences may follow.

Name: .....

Signature: ..... **Date:** .....

Appendix 2:

Responsible Use Agreement for Digital Leaders

- ☺ I will be a polite and helpful Digital Leader!
- ☺ I will make sure that I get my own work done as well as help my classmates.
- ☺ I will teach my classmates how to do something rather than just do it for them.
- ☺ I will keep all passwords and usernames a secret.
- ☺ When I am using the teacher's laptop I will never look at or click on any of the teacher's work.
- ☺ I will make sure the iPads and laptops are put away carefully and safely.
- ☺ I will check that the laptops are plugged in, charging and do not have any thing placed on top of them.
- ☺ I will let my teacher know if there are any problems with the iPads or laptops.

I WILL TRY MY BEST TO FOLLOW THESE RULES.

Pupil's signature: Class:

Appendix 3:

Online Safety: Personal Use of Social Media Policy

Introduction

This policy is one of a set of policies governing the conduct of employees of Sutton Veny CE Primary School. Social media is a type of interactive online communication that allows parties to communicate instantly with each other or to share information in a public forum. There are various online technology tools that enable people engage in social media.

This policy provides guidance to school employees who use social media sites in their personal time (either at home or during an authorised break at work), with the aim of protecting both staff and the school from disrepute.

The governing body of Sutton Veny CE Primary School has agreed to adopt this policy. The policy will be applied to all permanent, temporary and casual employees employed at the school.

This policy applies at all times when school employees are making use of social media sites in a personal capacity. It applies whether the employee is at home or at work and whether they are using school equipment or their own device.

This policy does not cover the use of social media sites by employees within their role on behalf of the school. Where employees use social media sites as part of their work the school will make them aware of the school's expectations and standards in the use of social media via that separate policy.

Social media etiquette

Social media allows people great freedom in how they communicate and express themselves. To help ensure everyone is able to equally benefit from social media sites, employees at Sutton Veny CE Primary School must abide by the following principles:

- tell the truth;
- write deliberately and with accuracy;
- acknowledge and correct mistakes promptly;
- preserve the original post, using notations to show where changes have been made, so as to maintain the integrity of any material published
- never delete someone else's post, although a poster could delete their own post.
- give due consideration when posting comments and have regard to the advice within this policy;
- strive for high quality with every post – including basic spellchecking;
- stay on topic;
- disagree with other opinions respectfully;
- link to online references and original source materials directly;
- disclose conflicts of interest;
- keep private issues and topics separate from work issues and topics.

Many employees make use of social media in a personal capacity and this policy is not intended to limit their use or enjoyment of social media. However, employees should remember that, even when not acting on the school's behalf, they can be held accountable for content which they post on social

media sites which could be potentially damaging to the school. Damaging content includes any communication made in a personal capacity through social media which:

Brings the school into disrepute	e.g. criticising the school, pupils or colleagues/governors in an inappropriate manner, posting images that are inappropriate or links to inappropriate content.
Breaches confidentiality	e.g. revealing information owned by the school; giving away confidential information about an individual (such as a colleague or pupil) or discussing the school's internal workings (such as school budget spending that have not been communicated to the public)
Is discriminatory against, or bullying or harassment of, any group or individual	e.g. making offensive or derogatory comments relating to sex, gender reassignment, race (including ethnicity), disability, sexual orientation, religion or belief or age; using social media to bully another individual; or posting images that are discriminatory or offensive, or links to such content.
Breaches copyright	e.g. by using someone else's images or written content without permission.

Employees:

- must consider who can read what is posted, they must be aware that some sites are open to all and other sites allow the employee to control who can see what has been posted
- must carefully consider, before posting content on social media sites, whether this will bring the school into disrepute, breach confidentiality or copyright or be considered offensive, defamatory, discriminatory, bullying or is potential harassment
- need to ensure that they have reviewed privacy settings so that only those who they wish to read the content are able to do so
- should not include their workplace and/or job title on their profile, being aware that this may make it easier for pupils, parents and members of the public to contact them in their personal time
- should make it clear that they are not representing the school when commenting in a personal capacity on any issues relating to the school, and that the views expressed are personal and do not necessarily reflect the views of the school
- may make occasional and reasonable personal use of the internet (for example during their lunch break), as long as this does not interfere with the performance of their duties or the work of other colleagues
- must only access social media sites for personal use on their own equipment (e.g. mobile phone, smartphone etc.) during official breaks

The school:

- will monitor social media websites in the same way as it monitors other media channels (e.g. local press etc.) for relevant content about the school
- will not routinely monitor the webpages that an employee can access from their school laptop, however full logs are retained and can be accessed as part of a genuine investigation
- does not monitor employee's personal social media pages without reason. However, as with any allegation of misconduct, the school will investigate where breaches of this policy are brought to its attention by any means

Investigation which involves social media content will take into consideration the intent of the content, what damage has been done, the implications, the impact and the individual's right to freedom of expression (provided it is not discriminatory, damaging, malicious or libellous).

Inappropriate content posted on social media sites either during, or outside of work time, may lead to either informal or formal disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues, discriminatory behaviour or social media activity causing serious damage to the school, may constitute gross misconduct and lead to summary dismissal. Social media content which proves that employees have breached other school policies may be used in disciplinary investigations relating to these matters.

This policy has been Equality Impact Assessed to identify opportunities to promote equality and mitigate any negative or adverse impacts on particular groups.

Legislation and guidance:

Human Rights Act 1998
Data Protection Act 1988
Equalities Act 2011
ACAS Factsheets "Social Networking"
Guidance for safer working practice for adults who work with children and young people in education settings

Further information:

There are a number of related policies and procedures that employees should be aware of including:
Code of Conduct
Dignity at work
Disciplinary policy and procedure
Grievance policy and procedure
Whistleblowing policy

In addition, employee's job descriptions may contain requirements relating to their conduct. There are also professional codes of conduct e.g. teacher's standards, that relate to the work an employee does and how it is done.

Appendix 4a:

Sutton Veny Responsible Use Agreement for KS1 Children

I will only go on websites that my teacher tells me to.

I will look after school computer equipment and tell a teacher straight away if something is broken or not working

I will always check with my teacher before printing.

I will tell my teacher straight away if I go on a website by mistake.

I will always tell a teacher if something makes me worried or unhappy.

I will shut down a computer when I have finished using it.

All my work on the computers and iPads will be polite and kind.

I understand that I must do my best to follow these rules.

Parent/Carer's Signature: _____ Date: _____

Child's Signature: _____

Appendix 4b:

Acceptable Use Agreement Policy for KS2 Children

☺ I will **always** look after the ICT equipment and not damage it in any way.

☺ I will ask permission from a member of staff before using the Internet.

☺ I will only visit websites to help me with schoolwork or homework or that my teacher has said I can go on.

☺ I will only send messages to people that my teacher has agreed to.

☺ The messages I send and the work I do will be polite and responsible, and not contain anything that might upset someone else.

☺ I will always use what I have learned about e-safety to keep myself safe and will tell a teacher if something makes me worried or unhappy.

☺ I will keep my usernames and passwords safe by not telling anyone else.

☺ I will not change any settings on the computers at school.

☺ I will tell an adult if there is something wrong with the computer and not try to fix it myself.

☺ I will only change or delete my own files.

☺ I will only look at other people's files or messages with their permission.

☺ I will always close down the computers properly after use.

I UNDERSTAND THAT I MUST FOLLOW THESE RULES.

Pupil's signature: Class:

Parent/Carer's signature: Date:

Appendix 5:

Acceptable Use Agreement for Community Users

This acceptable use agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential harm in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

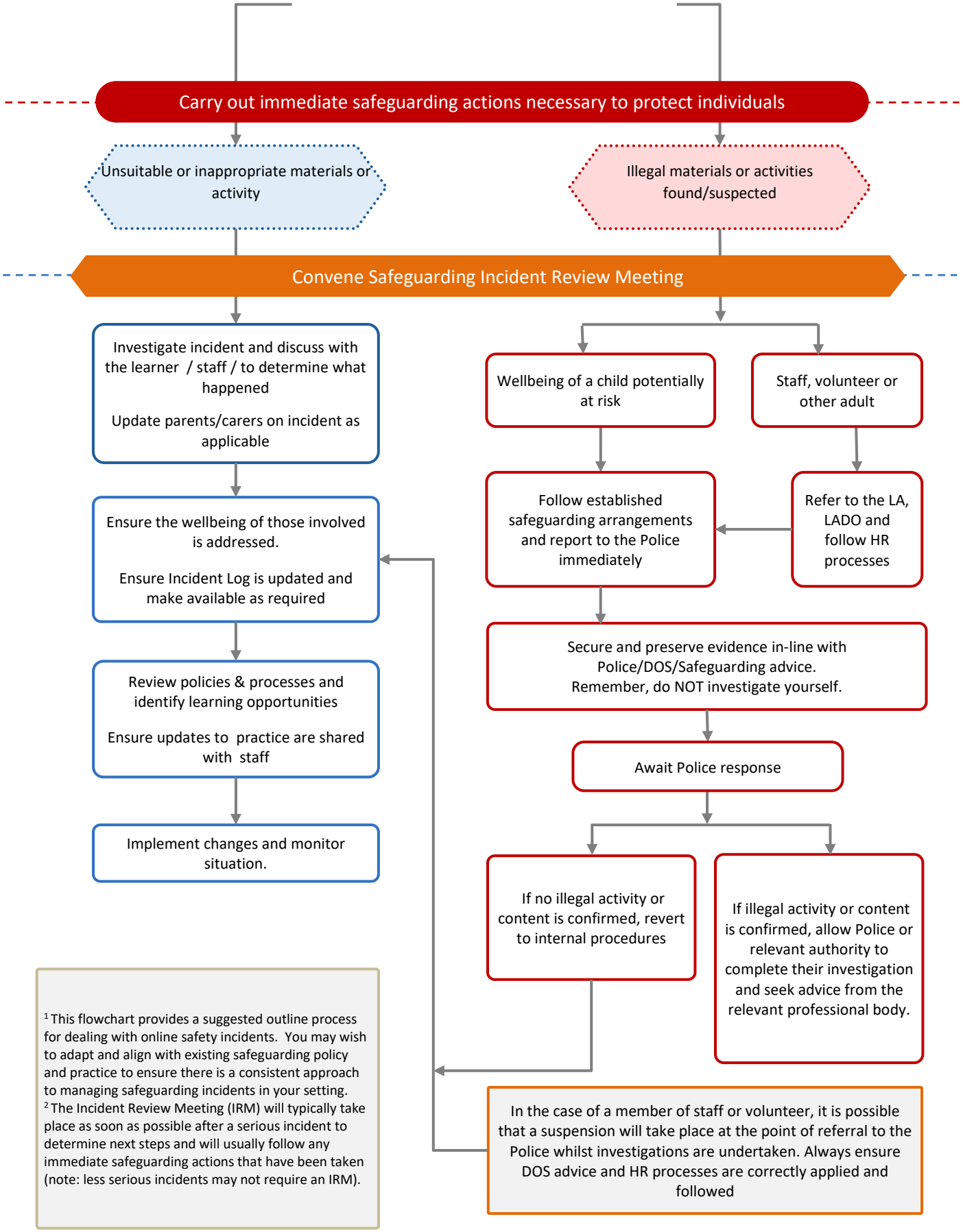
- I understand that my use of school systems and devices will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist and extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the Headteacher.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and/or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that if I fail to comply with this acceptable use agreement, the school/academy has the right to remove my access to school systems/devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name: ..... Signed: .....

Date : ……


Carry out immediate safeguarding actions necessary to protect individuals
Unsuitable or inappropriate materials or activity
Illegal materials or activities found/suspected
Convene Safeguarding Incident Review Meeting
Investigate incident and discuss with the learner / staff / to determine what happened
Update parents/carers on incident as applicable
Ensure the wellbeing of those involved is addressed.
Ensure Incident Log is updated and make available as required
Review policies & processes and identify learning opportunities
Ensure updates to practice are shared with staff
Implement changes and monitor situation.
Wellbeing of a child potentially at risk
Staff, volunteer or other adult
Follow established safeguarding arrangements and report to the Police immediately
Refer to the LA, LADO and follow HR processes
Secure and preserve evidence in-line with Police/DOS/Safeguarding advice.
Remember, do NOT investigate yourself.
Await Police response
If no illegal activity or content is confirmed, revert to internal procedures
If illegal activity or content is confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body.
In the case of a member of staff or volunteer, it is possible that a suspension will take place at the point of referral to the Police whilst investigations are undertaken. Always ensure DOS advice and HR processes are correctly applied and followed
[1] This flowchart provides a suggested outline process for dealing with online safety incidents. You may wish to adapt and align with existing safeguarding policy and practice to ensure there is a consistent approach to managing safeguarding incidents in your setting.
[2] The Incident Review Meeting (IRM) will typically take place as soon as possible after a serious incident to determine next steps and will usually follow any immediate safeguarding actions that have been taken (note: less serious incidents may not require an IRM).