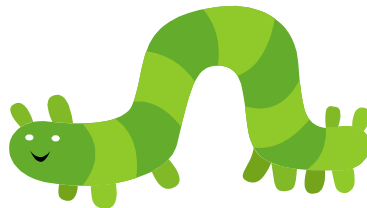




and



Abbots Farm Preschool

Online Safety Policy

November 2025

Review by November 2026

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Online Safety Policy Aims](#)
4. [Acceptable Use](#)
5. [Cyberbullying](#)
6. [Child-on Child Harmful Sexual Behaviour Online](#)
7. [Grooming and Exploitation](#)
8. [Online Hoaxes and Harmful Online Challenges](#)
9. [Reporting and Responding](#)
10. [School Actions](#)
11. [Cyber- Crime](#)
12. [Online Safety Education Programme](#)
13. [Staff Training](#)
14. [Governors](#)
15. [Parental Engagement and Partnership in Online Safety](#)
16. [Remote Learning](#)
17. [Technology](#)
18. [Filtering and Monitoring](#)
19. [Network Security](#)
20. [Emails](#)
21. [Generative Artificial Intelligence \(AI\)](#)
22. [Social Media](#)
23. [Digital and Video Images](#)
24. [Online Publishing](#)
25. [Data Protection](#)
26. [Monitoring and review](#)

Appendices

1. Responding to incidents of misuse – flow chart
2. Record of reviewing devices/internet sites (responding to incidents of misuse)
3. Reporting Log
4. Training Needs Audit Log
5. Links to other organisations or documents

Statement of intent

Abbots Farm Infant School and Abbots Farm Preschool understand that using online services is an important aspect of raising educational standards, promoting achievement, and enhancing teaching and learning.

We want our children to be able to understand and apply the key skills of computing.

Our children will develop skills enabling them to embrace a digital world. These include the knowledge and abilities to communicate in a variety of ways, solve problems logically and create and correct algorithms, using a wide range of digital technology, whilst knowing how to keep themselves safe online.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of children and staff.

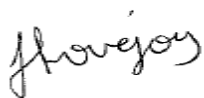
The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content:** Being exposed to illegal, inappropriate or harmful material, e.g. pornography, racism, misogyny, anti-Semitism, radicalisation, disinformation (including fake news), conspiracy theories, self-harm and suicide, and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages and images, and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images, and cyberbullying.
- **Commerce:** Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect children and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all children and staff.

Our Online Safety Lead is Mrs Lovejoy, who is supported by Mrs Hancock (Computing Lead).

Signed by:



Headteacher

Date: 25/11/25



Chair of governors

Date: 25/11/25

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- DfE 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies and procedures:

- Anti-Bullying Policy
- Allegations of Abuse Against Staff Policy
- Behaviour and Relationships Policy
- Confidentiality Policy
- Cyber Response and Recovery Plan
- Cyber-security Policy
- Data Protection Policy
- Disciplinary Policy and Procedure
- Low-level Safeguarding Concerns Policy
- PSHE and RSHE Policy
- Pupil Remote Learning Plan
- Safeguarding and Child Protection Policy
- Staff Code of Conduct
- Technology Acceptable Use Agreement for Pupils
- Technology Acceptable Use Agreement – Staff
- Whistleblowing Policy

2. Roles and responsibilities

The **Governing Body** is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.

- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for and responding to, online challenges and hoaxes embedded within them.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.
- Appointing an online safety Governor to meet regularly with the online safety Lead to monitor online safety incident and filtering logs and report to the governing body. Also to attend online safety training.

The **Headteacher and Senior Leaders** are responsible for:

- 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.
- 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 will receive regular monitoring reports from Securus and will check and act on these reports as necessary.
- Maintaining detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their safeguarding training.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping children safe.

The **Headteacher as Online Safety Lead** is responsible for:

- Being a DSL
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online including the potential for serious safeguarding issues to arise from:
 - sharing of personal data
 - access to illegal/inappropriate materials
 - inappropriate online contact with adults/strangers
 - potential or actual incidents of grooming
 - online bullying.
- Taking day-to-day responsibility for online safety issues, and being aware of the potential for serious child protection concerns.
- Having a leading role in establishing and reviewing the school online safety policies and documents.
- Promoting an awareness of and commitment to online safety education and awareness raising across the school and beyond.
- Liaising with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents.

- Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments.
- Providing (or identifying sources of) training and advice for staff, governors, parents/carers and learners.
- Liaising with WCC technical staff.
- Meeting regularly with the online safety governor to discuss current issues, review (anonymised) incidents and if possible, filtering and monitoring logs.
- Attending relevant governing body meetings.
- Reporting regularly to the governing body.
- Liaising with the local authority.

Curriculum leads are responsible for:

- Working with the Online Safety Lead to develop a planned and coordinated online safety education programme. This will be provided through:
 - A discrete online safety programme
 - A mapped cross-curricular programme
 - PSHE and RSHE programmes such as Jigsaw
 - Assemblies and pastoral programmes
 - Relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#).

All **staff members** are responsible for ensuring:

- They have an awareness of current online safety matters and trends and of the current school Online Safety Policy and practices.
- They understand that online safety is a core part of safeguarding.
- Ensuring they are familiar with, and understand, the indicators that children may be unsafe online.
- They immediately report any suspected misuse or problem to the **Headteacher** for investigation and action, in line with the school safeguarding procedures. If they suspect the Headteacher of misuse this must be reported to the **Chair of Governors** immediately.
- Maintaining a professional level of conduct in their personal use of technology. They have read, understood, and signed the staff acceptable use agreement (AUA).
- All digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Online safety issues are embedded in all aspects of the curriculum and other activities.
- They supervise and monitor the use of digital technologies, iPads, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices.
- In lessons where internet use is pre-planned learners should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Technical Support Staff from WCC supported by Online Safety Lead are responsible for ensuring that:

- They are aware of and follow the school Online Safety Policy and Security Policy to carry out their work effectively in line with school policy.

- The school technical infrastructure is secure and is not open to misuse or malicious attack.
- The school meets (as a minimum) the required online safety technical requirements as identified by the local authority.
- There is clear, safe, and managed control of user access to networks and devices.
- 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.
- The use of technology is regularly and effectively monitored in order that any misuse and attempted misuse can be reported to the **Headteacher** for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring software and systems are implemented and regularly updated as agreed in school policies.

Children are responsible for:

- Using the school digital technology systems in accordance with the Pupil Acceptable Use Agreement and Online Safety Policy.
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use online services and devices in an appropriate way. The school will take every opportunity to help parents and carers understand these issues through:

- Publishing the school Online Safety Policy on the school website
- Providing them with a copy of the learners' acceptable use agreement
- Publishing information about appropriate use of social media relating to posts concerning the school
- Seeking their permissions concerning digital images, cloud services etc.
- Parents' and carers' evenings, newsletters, website, social media and information about national and local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- ClassDojo and other on-line apps used for pupil records

3. Online Safety Policy Aims

The school Online Safety Policy:

- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Allocates responsibilities for the delivery of the policy.
- Is regularly reviewed in a collaborative manner, taking account of online safety incidents and changes and trends in technology and related behaviours.
- Establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard learners in the digital world.
- Describes how the school will help prepare learners to be safe and responsible users of online technologies.

- Establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms.
- Is supplemented by a series of related acceptable use agreements.
- Is made available to staff at induction and is on the OneDrive.
- Is published on the school website.

4. Acceptable Use

The school has defined what it regards as acceptable and unacceptable use and this is shown in the following tables.

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated and reinforced through:

- Staff induction and handbook
- Posters and notices around where technology is used
- Communication with parents and carers
- Integration into education sessions
- School website
- Peer support through the E-Safety Council

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: <ul style="list-style-type: none"> • Child sexual abuse imagery • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images e.g., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering 					X
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	<ul style="list-style-type: none"> • Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality 					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
	through the use of computers/devices <ul style="list-style-type: none"> Using penetration testing equipment (without relevant permission) 					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

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

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and children or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community.
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.

Consideration should be given for the following activities when undertaken for non-educational purposes:	Staff and other adults				Children			
	Not allowed	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission/awareness
Mobile phones may be brought to school		X			X			

Use of mobile phones for learning at school					X			
Use of mobile phones in social time at school		X			X			
Taking photos on mobile phones/cameras	X				X			
Use of other personal devices, e.g. tablets, gaming devices			X		X			
Use of personal e-mail in school, or on school network/wi-fi	X				X			
Use of school e-mail for personal e-mails	X				X			

5. Cyberbullying

Cyberbullying is when someone is unkind or hurtful to others using technology such as phones, tablets, or computers. This can include:

- Sending upsetting or threatening messages
- Sharing pictures or videos to embarrass someone
- Making silent or abusive phone calls
- Pretending to be someone else to send unkind messages
- Posting hurtful comments online or on social media

The school recognises that some children may be more vulnerable to online bullying, including those with special educational needs and disabilities (SEND), or those exploring their identity.

Cyberbullying of any kind is not tolerated at our school.

Any incidents involving pupils or staff will be dealt with promptly and in line with our Anti-Bullying Policy. We are committed to keeping all members of our school community safe, both offline and online.

6. Child-on Child Harmful Sexual Behaviour Online

While our children are young, staff are aware that inappropriate behaviour online can still occur and must be taken seriously. Children may use technology in ways that are harmful to others, including behaviours that are sexual in nature. These behaviours can happen both in and out of school, and may not always be reported by children, especially if they are using websites or apps that are not suitable for their age.

Staff will be alert to the following examples of harmful online behaviour:

- Sharing or encouraging inappropriate or sexual content
- Taking or sharing images without permission
- Making rude or upsetting jokes or comments
- Sending unwanted messages that make others feel uncomfortable
- Sharing pictures or videos that are not appropriate for their age

All staff will promote a zero-tolerance approach to any behaviour that is sexually inappropriate or harmful. It is important that such behaviour is never dismissed as “just a joke” or “harmless fun,” as this can lead to a culture where abuse is normalised and children feel unable to speak up.

Staff will also be aware that creating, sharing, or possessing inappropriate images of children under 18 is a criminal offence, even if the child involved gives permission or shares the image themselves.

If any concerns arise, including those involving social media or online interactions between children, they will be reported to the Designated Safeguarding Lead (DSL). The school will respond in line with the Safeguarding and Child Protection Policy, regardless of where or how the incident occurred.

7. Grooming and Exploitation

Grooming is when an adult tries to build a close relationship with a child to trick or hurt them. This can happen online, and children may not always tell someone because they might feel confused, scared, or even think the adult is their friend.

Staff will be trained to spot signs that a child might be experiencing grooming online, such as:

- Being secretive about what they do online
- Talking about older friends that others haven't met
- Having new things like clothes or gadgets they can't explain

Child Sexual Exploitation (CSE) can involve children being pressured or tricked into doing things that are not appropriate, sometimes through the internet. This can include being asked to share pictures or videos or being made to act in ways that are harmful.

Child Criminal Exploitation (CCE) is when children are used by others to commit crimes, such as stealing or carrying things for others. This can also start online, where children are persuaded or threatened into doing things they wouldn't normally do.

Any concerns about grooming, CSE, or CCE must be reported to the Designated Safeguarding Lead (DSL) immediately. The DSL will follow the school's **Safeguarding and Child Protection Policy**.

Radicalisation

Radicalisation is when someone tries to get a child to support dangerous or extreme ideas, including terrorism. This can happen online, where children may be shown videos or messages that try to change how they think or feel.

Staff will be aware of the signs that a child may be at risk and will follow the **Prevent Duty**. If a child is showing signs of radicalisation, staff must report it to the DSL straight away. The DSL will respond according to the **Safeguarding and Child Protection Policy**.

8. Online Hoaxes and Harmful Online Challenges

Staff will be aware that children may come across online hoaxes — false stories or messages shared online that are designed to scare or upset people. These are often spread through social media and can be confusing or distressing for young children.

Staff will also be aware of online challenges, where children are encouraged to record themselves doing something and share it online. While many challenges are harmless, some can be dangerous or upsetting, especially if they involve risky behaviour or sharing videos that are not appropriate for the child's age.

If staff suspect that a harmful challenge or hoax is being shared among pupils, they must report it to the **Designated Safeguarding Lead (DSL)** immediately.

The DSL will:

- Assess the risk and decide how serious the issue is
- Consider whether the problem is local or more widespread
- Work with the local authority if needed to help stop the spread

Before responding, the DSL will carefully consider:

- Advice from trusted sources (e.g. UK Safer Internet Centre)
- Whether the response might cause unnecessary worry
- Whether talking about the issue might make children more curious
- Whether the response is suitable for the age and understanding of the pupils
- How to support any pupils who may be affected
- Whether the response fits with the **Safeguarding and Child Protection Policy**

If the DSL finds that a challenge is putting children at risk, they will make sure the right pupils are spoken to — either individually or in small groups — depending on the situation.

A whole-school response will only be used if it is safe and appropriate to do so, and if the risk of increasing exposure to the harmful content has been carefully considered and reduced.

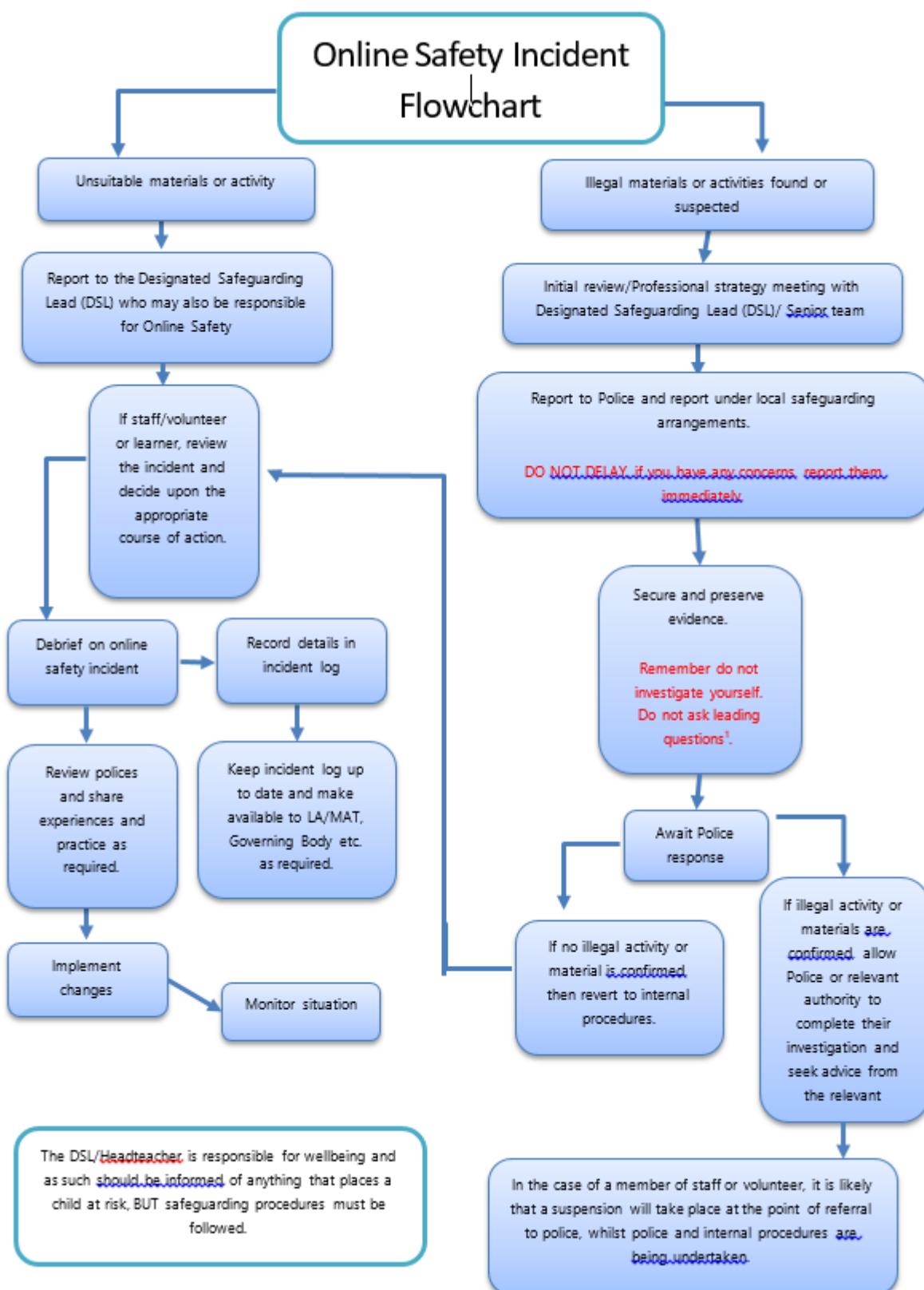
9. Reporting and Responding

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.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm ([see flowchart and user actions chart in the appendix](#)), the incident must be escalated through the agreed school safeguarding procedures.
- Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors.
- Where there is no suspected illegal activity, devices can be checked using the following procedures:
 - one or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
 - conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
 - ensure that the relevant staff 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, signed, and attached to the form (Appendix 2)

- 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
- That those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- Incidents will be logged **(See Reporting Log Appendix 3).**
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; [Professionals Online Safety Helpline](#); [Reporting Harmful Content](#); [CEOP](#).
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant).
- Learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Senior Leadership Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - children, through assemblies/lessons
 - parents/carers, through newsletters, school social media, website
 - governors, through regular safeguarding updates
 - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



10. School Actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour procedures as follows:

10.1 Responding to Learner Actions

Incidents	Refer to class teacher	Refer to Headteacher	Refer to Police	Refer to local authority technical support for advice/action	Inform parents/carers	Remove device/ network/internet access rights	Issue a warning	Further sanction, in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X		x			
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X		X		X	
Corrupting or destroying the data of other users.	X				X			X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature		X	X		X	X	X	X
Unauthorised downloading or uploading of files or use of file sharing.	X							
Using proxy sites or other means to subvert the school's filtering system.		X	X	X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident.		X						
Deliberately accessing or trying to access offensive or pornographic material.		X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.		X	X	X	X	X	X	X
Unauthorised use of digital devices (including taking images)	X							
Unauthorised use of online services	X							

Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.		X			X	X	X	X
Continued infringements of the above, following previous warnings or sanctions.			X			X		X

10.2 Responding to Staff Actions

Incidents	Refer to Headteacher	Refer to local authority	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	X	X	X	X			X
Deliberate actions to breach data protection or network security rules.	X	X	X	X			X
Deliberately accessing or trying to access offensive or pornographic material		X	X	X			X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X				X
Using proxy sites or other means to subvert the school's filtering system.	X	X		X			X
Unauthorised downloading or uploading of files or file sharing	X			X	X		X
Breaching copyright or licensing regulations.	X	X	X		X		X
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account.	X				X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X				X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/carers	X	X	X				X
Inappropriate personal use of the digital technologies e.g. social media / personal e-mail	X			X	X		X
Careless use of personal data, e.g. displaying, holding or transferring data in an insecure manner	X	X			X		X
Actions which could compromise the staff member's professional standing	X	X	X				X
Actions which could bring the school							

into disrepute or breach the integrity or the ethos of the school.	X	X					X
Failing to report incidents whether caused by deliberate or accidental actions	X						X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X

11. Cyber- Crime

Cyber-crime refers to illegal activity carried out using computers or the internet. There are two main types:

- **Cyber-enabled crimes** – These are crimes that can happen offline but are made easier or more widespread online, such as fraud or the sharing of illegal content.
- **Cyber-dependent crimes** – These can only happen online or through the use of computers, such as hacking or creating harmful software.

Although our pupils are young, the school recognises that some children may show a strong interest or skill in technology. Staff will be aware that, in rare cases, this could lead to children becoming involved in cyber-crime, either knowingly or by accident.

If staff have concerns about a pupil's use of technology or their intentions, they will report this to the **Designated Safeguarding Lead (DSL)**. The DSL may consider a referral to the **Cyber Choices programme**, which helps guide children towards using their skills in positive and safe ways.

The headteacher and Computing Lead will ensure that pupils are taught, through the curriculum, how to use technology safely, responsibly, and legally.

12. Online Safety Education Programme

Our school's approach to online safety education reflects the ever-changing nature of digital risks. We aim to equip children with the knowledge, skills, and resilience to navigate online spaces safely and responsibly. Online safety is embedded across the curriculum and reinforced by all staff, ensuring consistent messaging and a whole-school approach.

Curriculum Integration and Delivery

Online safety is a focus in all areas of learning. Staff are expected to reinforce online safety messages throughout the curriculum, not just in dedicated lessons. The online safety curriculum is broad, relevant, and progressive, offering creative and engaging learning opportunities. It is delivered in the following ways:

- A **planned online safety curriculum** using *Purple Mash* for Key Stage 1, aligned with a nationally agreed framework and taught regularly in varied contexts.
- Lessons are **age-appropriate**, matched to pupils' needs, and build on prior learning.
- Content is **context-relevant**, with clear objectives and measurable outcomes.
- Planning and assessment ensure that **children's needs and progress** are effectively addressed.
- **Digital competency** is integrated into other subjects such as PSHE and English.
- National initiatives like **Safer Internet Day** and **Anti-Bullying Week** are incorporated to enhance learning.
- The programme is **accessible to all children**, including those with additional learning needs or English as an additional language.
- Children are supported to understand and follow the **Pupil Acceptable Use Agreement**, promoting safe and responsible behaviour both in and out of school.
- Staff act as **positive role models** in their use of digital technologies, the internet, and mobile devices.

- In lessons with planned internet use, children are guided to **pre-checked, age-appropriate websites**, and procedures are in place to manage any unsuitable content.
- When children are allowed to search the internet freely, staff maintain **vigilant supervision** and monitor website content.
- The online safety programme is kept **up to date and relevant**, ensuring high-quality learning and outcomes.

Key Risk Areas

Online safety education addresses four key categories of risk:

Content Risks

Children learn to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. Topics include misinformation, fake news, and harmful content such as racism, extremism, and self-harm. Children are taught to question sources, verify information, and understand the risks of engaging with such content.

Contact Risks

Children are educated about the dangers of online interactions, including peer pressure, exploitation, and grooming. They learn to recognise unsafe behaviour, use privacy settings, and report concerns to trusted adults or platforms.

Conduct Risks

Children explore how their online behaviour affects themselves and others. Lessons cover online bullying and the risks of sharing personal or inappropriate images. Children are taught responsible digital conduct and the consequences of harmful behaviour.

Commerce Risks

Children are informed about online commercial risks such as gambling, advertising, and scams. They learn to identify fraudulent schemes, protect personal information, and seek help when needed.

Safeguarding and Support

The **Designated Safeguarding Lead (DSL)** plays a key role in developing and supporting the online safety curriculum. Before lessons, staff will consider whether any children may have experienced online harm and plan accordingly. The DSL will advise on how to support affected children and ensure lessons are delivered sensitively.

Lessons are designed to avoid drawing attention to individual children who may have been harmed online. Teachers create a safe environment where pupils feel comfortable asking questions and expressing concerns.

Any concerns raised during lessons are reported in line with the **Safeguarding and Child Protection Policy**. Disclosures of online abuse are handled according to established procedures.

13. Staff Training

All staff will receive training in online safety and understand their responsibilities as outlined in this policy. The **Designated Safeguarding Lead (DSL)** will ensure that all safeguarding training includes key aspects of online safety, such as how the internet can be used to facilitate abuse or exploitation, and the roles staff play in managing filtering and monitoring systems.

Staff will be made aware that children can be at risk of abuse both online and offline, and that these risks often occur at the same time. Training will help staff recognise harmful online narratives, including misinformation, disinformation, and conspiracy theories, and understand how these may affect children and families.

Training Programme

Online safety training will be delivered through a structured and ongoing programme:

- A **planned programme of formal training** in online safety and data protection will be available to all staff, regularly updated and reinforced.
- An **audit of staff training needs** will be carried out regularly to ensure everyone receives the support they need.
- Online safety training will be a **core part of the school's annual safeguarding and data protection training**.
- **New staff** will receive online safety training as part of their induction, covering the school's policy, acceptable use agreements, classroom management, professional conduct, online reputation, and modelling positive online behaviours.
- The **Online Safety Lead** will stay informed through external training events and by reviewing guidance from trusted organisations.
- This policy and any updates will be **shared and discussed in staff meetings**.
- The Online Safety Lead will offer **advice, guidance, and individual training** as needed.

Training will give staff the confidence and knowledge to:

- Identify signs of online harm.
- Respond appropriately to disclosures or concerns.
- Support pupils in developing safe online habits and critical thinking skills.

14. Governors

Governors should take part in online safety training and awareness sessions, with particular importance for those who are involved in technology and online safety, health and safety and safeguarding. This may be offered in several ways such as:

- Attendance at training provided by the local authority.
- Participation in school training and information sessions for staff or parents.

A higher level of training will be made available to (at least) the Online Safety Governor.

15. Parental Engagement and Partnership in Online Safety

The school is committed to working in close partnership with parents and carers to ensure pupils remain safe online both at school and at home. We aim to raise awareness and provide support through a variety of channels and initiatives:

- **Regular Communication:** Parents and carers will receive ongoing updates and guidance on online safety through letters, newsletters, the school website, and ClassDojo posts.
- **Workshops and Events:** Opportunities for engagement will include awareness workshops and high-profile campaigns such as Safer Internet Day.
- **Curriculum Integration:** Children are encouraged to share online safety messages learned in class with their families, reinforcing key principles at home.
- **Resources and Guidance:** Parents will be directed to trusted resources such as SWGfL, <https://www.saferinternet.org.uk>, and <https://www.childnet.com/parents-and-carers> (see Appendix 5 for further links).
- **Consortium Collaboration:** Good practice will be shared with other schools in our Consortium and Soft Federation to strengthen collective efforts.

- **Acceptable Use Agreement:** At the start of each academic year, parents will receive a copy of the school's Acceptable Use Agreement and are encouraged to review it with their child to ensure understanding and compliance.
- **Risk Awareness:** Parents will be informed about potential online risks, including:
 - Child sexual abuse and grooming
 - Exposure to radicalising content
 - Sharing of indecent imagery (e.g. sexting)
 - Cyberbullying
 - Age-inappropriate content (e.g. pornography)
 - Harmful content (e.g. self-destructive behaviour)
- **Home Safety Measures:** Guidance will be provided on implementing parental controls and other strategies to prevent access to harmful content at home.
- **Support Channels:** Parental awareness will be further supported through workshops, newsletters, and curated online resources.

16. Remote Learning

All remote learning is delivered in line with the school's Pupil Remote Learning Plan.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

17. Technology

The school is responsible for ensuring that the school infrastructure and network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The school should ensure that all staff are made aware of policies and procedures in place on a regular basis and explain that everyone is responsible for online safety and data protection.

18. Filtering and Monitoring

The governing body will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The governing body will ensure 'over blocking' does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The school filtering policies are agreed by senior leaders and WCC technical staff and are regularly reviewed and updated in response to changes in technology and patterns of online safety incidents and behaviours.

The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre [Appropriate filtering and](#) the DfE's '[Filtering and monitoring standards for schools and colleges](#)'.

The headteacher will ensure the filtering and monitoring systems the school implements will be appropriate to children's ages, the number of children using the network, how often children access the network, and the proportionality of costs compared to the risks. The Headteacher will undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Prior to making any changes to the filtering system, the Headteacher will conduct a risk assessment. Any changes made to the system will be recorded. Reports of inappropriate websites or materials will be made to the Headteacher immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL, who will escalate the matter appropriately. If a child has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Safeguarding and Child Protection Policy.

19. Network Security

The 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 are securely located and physical access restricted.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud.
- All users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually, by the Senior Leadership Team.
- All users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by Lydia Mortimer (School Business Manager) who will keep an up-to-date record of users and their usernames
- The master account passwords for the school systems are kept in a secure place.
- Passwords should be at least 8 characters long and contain upper and lower case letters, digits and symbols.

- Records of learner usernames and passwords for learners in Key Stage 1 or younger can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user.
- Jeanette Lovejoy (Headteacher) is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- An appropriate system is in place for users to report any actual or potential technical incident or security breach to the Headteacher.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices 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 workstations are protected by up-to-date endpoint (anti-virus) software.
- Lydia Mortimer (School Business Manager) will set up temporary access of 'guests', (e.g., trainee teachers, supply teachers, visitors) onto the school systems. Jeanette Lovejoy (Headteacher) will give access to programmes needed to do their job.
- An agreement is in place regarding the extent of personal use that users (staff and children) and their family members are allowed on school devices that may be used out of school.
- Staff must seek permission from headteacher before downloading executable files and installing programmes on school devices.
- Staff are allowed to use removable media (e.g., memory sticks/CDs/DVDs) on school devices. Where possible these should be encrypted.
- Systems are in place that prevent the unauthorised sharing of personal data unless safely encrypted or otherwise secured. (See Data Protection Policy for further details).

20. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy, Acceptable Use Agreement, and the Pupil Confidentiality Policy and Staff Code of Conduct.

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to WCC ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Staff will receive training on what a phishing email and other malicious emails might look like – the training will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking "does the email urge you to act immediately?"
- The importance of checking the spelling and grammar of an email

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

21. Generative Artificial Intelligence (AI)

As part of our commitment to preparing pupils for the digital world, the school will introduce age-appropriate awareness of emerging technologies, including generative AI, in a safe and responsible way.

- The school will ensure that pupils are supported to understand how to use new technologies safely, with teaching tailored to their age and level of understanding.
- Our IT systems will include appropriate filtering and monitoring to prevent access to or creation of harmful or inappropriate content using generative AI tools.
- Staff will take steps to ensure pupils do not access or produce harmful or inappropriate content through any digital platform, including generative AI.
- Personal and sensitive information will not be entered into generative AI tools, and pupils will be taught the importance of keeping personal data private.
- The school will follow trusted guidance and best practice to ensure a secure and safe foundation is in place before introducing more advanced technologies like generative AI.

22. Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to children through:

- Ensuring that personal information is not published
- Education and training being provided including acceptable use, age restrictions, social media risks, use of digital and video images, checking of settings, data protection and reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Guidance for children, parents and carers

School staff should ensure that:

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

On official school social media accounts, there is:

- A process for approval by senior leaders
- Clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts
- Systems for reporting and dealing with abuse and misuse
- Understanding of how incidents may be dealt with under school disciplinary procedures.

22.1 Personal use

- Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts upon the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.

22.2 Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.
- When parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

23. Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and children 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 available 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 inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff will inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images.
- Staff/volunteers must be aware of those children whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff should not be used for such purposes.
- In accordance with [guidance from the Information Commissioner's Office](#), parents/carers are welcome to take photographs of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites.
- Staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, storage, distribution and publication of those images.
- Care should be taken when sharing digital/video images that children are appropriately dressed.
- Children must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with Online Safety Policy.
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission is obtained from parents/carers on School Enrolment Forms to allow photographs of children to be taken for use in school or published on the school website/social media.
- Parents/carers will be informed of the purposes for the use of images, how they will be stored and for how long – in line with the school data protection policy.
- Images will be securely stored in line with the school retention policy.

24. Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Class Dojo

- Online newsletters

The school website is managed/hosted by Different Class. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.

Where children's work, images or videos are published, their identities are protected, and full names are not published.

On the schools website there is an E-Safety page which provides information about online safety e.g., Online Safety Policy and acceptable use agreements; curating latest advice and guidance; news articles etc.

25. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The school:

- Has a Data Protection Policy.
- Implements the data protection principles and can demonstrate that it does so.
- Has paid the appropriate fee to the Information Commissioner's Office (ICO).
- Has appointed an appropriate Data Protection Officer (DPO) through Warwickshire's DPO Service who has effective understanding of data protection law and is free from any conflict of interest. Our Data Controllers are Jeanette Lovejoy (Headteacher) and Lydia Mortimer (School Business Manager).
- Has a 'Record of Processing Activities' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it. The Record of Processing Activities lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis is listed.
- Has an 'information asset register' in place and knows exactly what personal data is held, where, why and which member of staff has responsibility for managing it. The information asset register lists the lawful basis for processing personal data (including, where relevant, consent). Where special category data is processed, an additional lawful basis will have also been listed.
- Will hold the minimum personal data necessary to enable it to perform its function and will not hold it for longer than necessary for the purposes it was collected for. The school 'retention schedule' supports this.
- Data held is accurate and up to date and is held only for the purpose it was held for. Systems are in place to identify inaccuracies, such as asking parents to check emergency contact details at suitable intervals.
- Provides staff, parents, governors and volunteers, with information about how the school looks after their data and what their rights are in a clear Privacy Notice.
- Has procedures in place to deal with the individual rights of the data subject.
- Carries out Data Protection Impact Assessments (DPIA) where necessary e.g. to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier.
- Has undertaken appropriate due diligence and has data protection compliant contracts in place with any data processors.
- Understands how to share data lawfully and safely with other relevant data controllers.

- Has clear and understood policies and routines for the deletion and disposal of data.
- Reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach as required by law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents.
- Has a Freedom of Information Policy which sets out how it will deal with FOI requests.
- Provides data protection training for all staff at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff.

When personal data is stored on any mobile device or removable media the:

- Data will be encrypted, and password protected.
- Device will be password protected.
- Device will be protected by up-to-date endpoint (anti-virus) software
- Data will be securely deleted from the device, in line with school policy once it has been transferred or its use is complete.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school.
- Can help data subjects understand their rights and know how to handle a request whether verbal or written and know who to pass it to in the school.
- Only use encrypted data storage for personal data.
- Will not transfer any school personal data to personal devices.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption, a secure email account (where appropriate), and secure password protected devices.

26. Monitoring and review

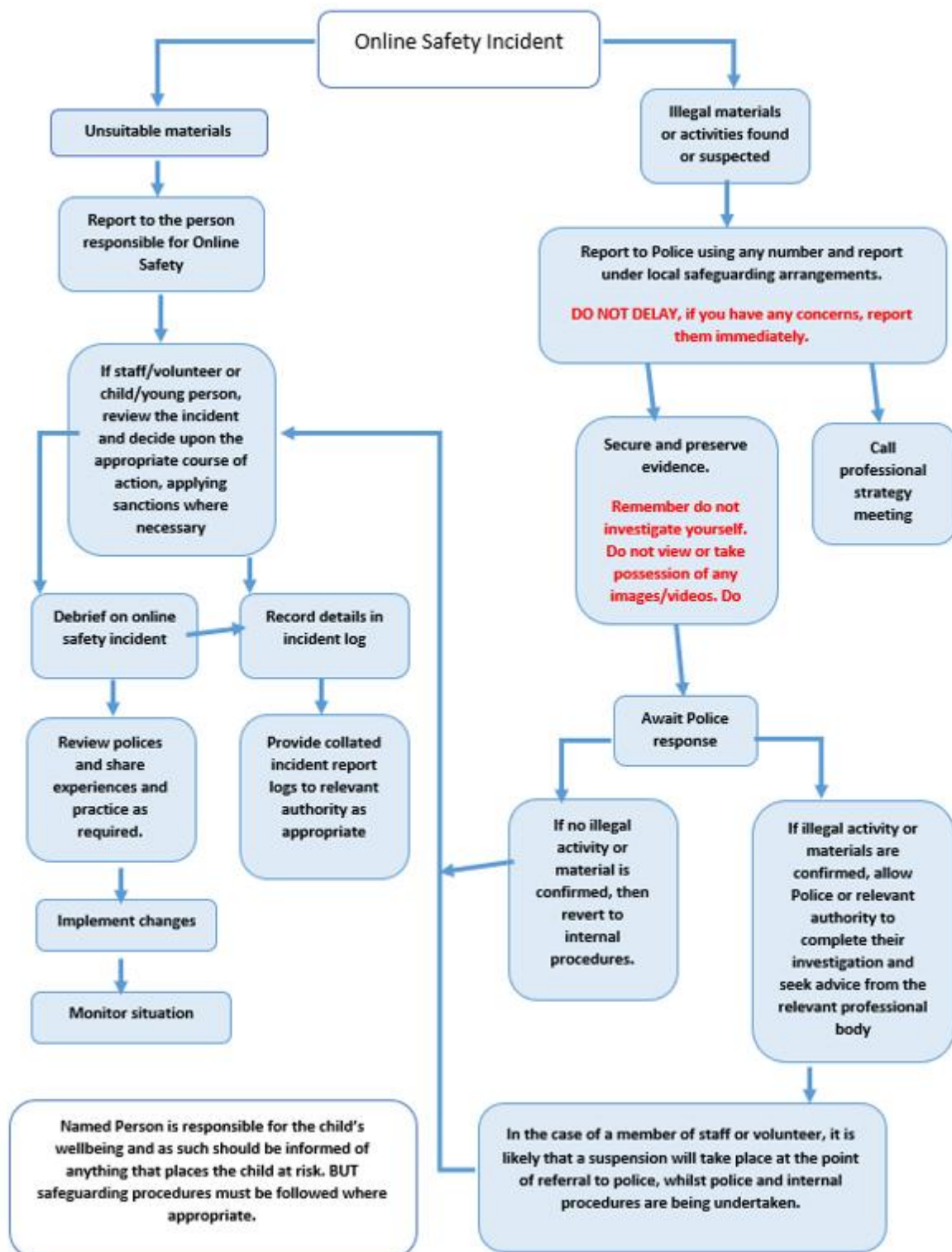
The **Governing Body, Headteacher** and **Computing Lead** review this policy in full on an **annual** basis and following any online safety incidents.

The school recognises that the online world is constantly changing; therefore, the headteacher will conduct light-touch reviews of this policy throughout the year to evaluate its effectiveness.

The next scheduled review date for this policy is **November 2026**.

Any changes made to this policy are communicated to all members of the school community.

Appendix 1: Responding to incidents of misuse – flow chart



Appendix 2: Record of reviewing devices/internet sites (responding to incidents of misuse)

Device:

Date:

Reason for investigation:

Details of first reviewer

Name:

Position:

Signature:

Details of second reviewing person

Name:

Position:

Signature:

Name and location of computer used for review (for web sites)

<i>Website(s) address/device</i>	<i>Reason for concern</i>

Conclusion and Action proposed or taken

Reporting Log

Group:

Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		

Appendix 3:

Training Needs Audit Log

Group:

Relevant training the last 12 months	Identified Training Need	To be met by	Cost	Review Date

Appendix 4:

Appendix 5: Links to other organisations or documents

The following links may help those who are developing or reviewing a school online safety policy and creating their online safety provision:

UK Safer Internet Centre

Safer Internet Centre – <https://www.saferinternet.org.uk/>

South West Grid for Learning - <https://swgfl.org.uk/online-safety>

Childnet – <https://www.childnet.com>

Professionals Online Safety Helpline - <https://saferinternet.org.uk/professionals-online-safety-helpline>

Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>

Internet Watch Foundation - <https://www.iwf.org.uk/>

Report Harmful Content - <https://reportharmfulcontent.com/>

[Harmful Sexual Support Service](#)

CEOP

CEOP - <https://www.ceop.police.uk>

ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

[LGfL – Online Safety Resources](#)

[Kent – Online Safety Resources page](#)

INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>

UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Tools for Schools / other organisations

Online Safety BOOST – <https://boost.swgfl.org.uk/>

360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>

SWGfL Test filtering - <http://testfiltering.com/>

UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>

[SWGfL 360 Groups – online safety self review tool for organisations working with children](#)

[SWGfL 360 Early Years - online safety self review tool for early years organisations](#)

Bullying/Online-bullying/Sexting/Sexual Harassment

Enable – European Anti Bullying programme and resources (UK coordination/participation through SWGfL & Diana Awards) - <http://enable.eun.org/>

SELMA – Hacking Hate - <https://hackinghate.eu/>

Scottish Anti-Bullying Service, Respectme - <https://respectme.org.uk/>

Scottish Government - Better relationships, better learning, better behaviour - <https://www.gov.scot/publications/developing-positive-whole-school-ethos-culture-relationships-learning-behaviour/>

DfE - Cyberbullying guidance - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

Childnet – Cyberbullying guidance and practical PSHE toolkit:

<https://www.childnet.com/what-we-do/our-projects/cyberbullying-guidance-and-practical-toolkit/>

[Childnet – Project deSHAME – Online Sexual Harrassment](#)

[UKSIC – Sexting Resources](#)

[Ditch the Label – Online Bullying Charity](#)

[Diana Award – Anti-Bullying Campaign](#)

Social Networking

UKSIC - [Safety Features on Social Networks](#)

[Children's Commissioner, TES and Schillings – Young peoples' rights on social media](#)

Curriculum

Purple Mash – access through <https://www.welearn365.com/>

SWGfL Evolve - <https://projectevolve.co.uk>

[UKCCIS – Education for a connected world framework](#)

Department for Education: Teaching Online Safety in Schools

Teach Today – <https://www.teachtoday.de/en/>

Data Protection

[ICO Guides for Organisations](#)

[IRMS - Records Management Toolkit for Schools](#)

[ICO Guidance on taking photos in schools](#)

Professional Standards/Staff Training

[DfE – Keeping Children Safe in Education](#)

DfE - [Safer Working Practice for Adults who Work with Children and Young People](#)

[UK Safer Internet Centre Professionals Online Safety Helpline](#)

Infrastructure/Technical Support/Cyber-security

[UKSIC – Appropriate Filtering and Monitoring](#)

[SWGfL Safety & Security Resources](#)

SWGfL - [Cyber Security in Schools](#).

NCA – [Guide to the Computer Misuse Act](#)

NEN – [Advice and Guidance Notes](#)

Working with parents and carers

[SWGfL – Online Safety Guidance for Parents & Carers](#)

[Vodafone Digital Parents Magazine](#)

[Childnet Webpages for Parents & Carers](#)

[Get Safe Online - resources for parents](#)

[Teach Today - resources for parents workshops/education](#)

[Internet Matters](#)

Prevent

[Prevent Duty Guidance](#)

[Prevent for schools – teaching resources](#)

Childnet – [Trust Me](#)