WREN PARK PRIMARY SCHOOL

WREN PARK

ONLINE SAFETY/ MOBILE & SMART TECHNOLOGY POLICY

RESPECTFUL AMBITIOUS RESILIENT

Policy Name:	Online Safety/ Mobile & Smart Technology Policy
This Online Safety Policy was approved by the governing body in:	May 2021
The implementation of this Online Safety Policy will be monitored by:	DSL, online safety lead, senior leadership team in conjunction with LinkICT.
Reviewed & Ratified by FGB	Pending: 23/01/2025
The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new technological developments, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2026

Should serious online safety incidents take place, the following external persons/agencies should be informed and further advice sought:	Derby Safeguarding Board, Police, LADO, CofG

Introduction

As we live in an increasingly digital age, especially since the advances during the pandemic and more recently within the field of AI, it is important that children have the skills necessary for their future education and employment in a technologically advanced world. It is also important to recognise the constant and fast paced evolution of technology within our society as a whole. Whilst exciting and beneficial both in and out of the context of education, there are also inherent risks with using technologies which access the internet. Children will face hazards and risks, which cannot be policed or prohibited; therefore, we aim to educate children to become discerning internet users who are aware of how to keep themselves safe and access the support of trusted adults. Our curriculum teaches children how to evaluate content, conduct themselves in a safe and appropriate manner as well as to ensure any contacts are agreed to be safe and known in real life. In addition, with the development of apps for children which have advertising, gambling with virtual coins and advertising aimed to gain financial reward from the parents, it is important children are aware of these risks and how to navigate the digital world. The teaching of appropriate behaviours and critical thinking enables them to remain both safe and within legal boundaries when using the Internet and related technologies in and beyond the context of the classroom. Within school, we foster an environment of open conversations, which enables risks to be identified and discussed. In addition, we recognise that children use the internet more predominately at home, especially during the pandemic; therefore, we provide support for parents in the use of parental controls, having open conversations and make informed choices about new and emerging apps and devices through workshops and website resources. Due to the higher risk to children with special educational needs and disabilities, we have dedicated resources, newsletters and support for these vulnerable groups.

Scope of the Online Safety Policy

This Online Safety Policy outlines the commitment of Wren Park Primary School to safeguard members of our school community online in accordance with statutory guidance (e.g. Keeping Children Safe in Education, Education for a Connected World etc.) and best practice. This is part of our wider approach to curriculum and safeguarding in addition to relating to other policies including those for Behaviour/ Relational Policy, Curriculum, Anti-bullying, Safeguarding and Child Protection.

This Online Safety Policy has been written in collaboration with relevant subject co-ordinators, Senior Leadership including the Headteacher and DSL, governors as well the children.

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

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

1. Aims

Our school aims to:

- have robust policies and processes in place to ensure the online safety of pupils, staff, volunteers, governors and the wider school community
- allocate clear responsibilities for the delivery of the policy
- set expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- have robust and effective monitoring and filtering systems to provide children with the safest environment possible (although it cannot ever be fully safe)
- ensure these systems are regularly reviewed and updated in a collaborative manner taking account of evidence gathered from these reviews/ audits/ professional debate online safety incidents and changes/trends in technology and related behaviours, as well as the local online safety strategy.
- establish clear mechanisms and responsibilities to identify, intervene and, if appropriate, escalate an incident
- throughout all online policies and procedures, the welfare of the child is paramount. Although children are often curious and may try to access material which is unsuitable, an incident may also raise safeguarding concerns for the child which need exploring. Children may be provided with emotional support, parents notified if appropriate, referrals to other services as well as in school support
- 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
- deliver an effective curriculum for online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile, smart and emerging technology

Our approach to online safety, in both learning and safeguarding, is based on addressing the four areas of risk:

- ***Content –*** being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- ***Contact*** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure including child-on child abuse, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes

- ***Conduct*** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nude and/or pornography), sharing other explicit images and online bullying, conduct relating to creating or sharing deep fakes.

- ***Commerce*** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

To ensure the online safeguarding of members of our school community, we aim to develop an ethos of working together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

3.1 The governing body

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This review will be carried out by the responsible governor who will receive regular information about online safety incidents and monitoring reports. The duties of the responsible governor to include:

- receiving training to enable the governors to check that the school meets the DfE Cyber-Security Standards
- regularly receiving reports of online safety incidents
- regular checking of the filtering and monitoring systems within school and ensuring this is recorded in the online filtering and safeguarding monitoring, recording and action log
- checking that provision outlined in the Online Safety Policy (e.g. online safety education provision and staff training) is taking place as intended

- ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) in line with the DfE Filtering and Monitoring Standards
- ensuring that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- Reporting back to the governing body

3.2 Headteacher and senior leaders

- The headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding, though the day-to-day responsibility for online safety is held by the Designated Safeguarding Lead, as defined in Keeping Children Safe in Education.
- The headteacher ensures all policies and procedures are followed and all statutory duties are met as well as overseeing the responsibilities of relevant staff (including our IT provider) are carrying out their duties effectively having received suitable training to enable them to carry out their roles consistently and effectively
- The headteacher, who is the Designated Safeguarding Lead, receives monitoring information to highlight trends, activities.
- The headteacher/senior leaders will work with the responsible Governor, the designated safeguarding lead (DSL) and IT service providers in all aspects of filtering and monitoring.
- The School Business Manager is responsible for recording any incidents or issues reported, as well as any Smoothwall breaches to the IT provider for system maintenance.
- The SBM contributes to weekly meetings with the DSL/headteacher and IT provider to identify any issues.

3.3 Designated Safeguarding Lead (DSL)

The DSL (who is also the headteacher), holds the lead responsibility for online safety, within their safeguarding role. They:

- receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online.
- meets regularly with the responsible governor to discuss current issues, review (anonymised) incidents and filtering and monitoring logs and ensuring that annual (at least) filtering and monitoring checks are carried out.
- is responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded
- Discuses weekly in meetings with the SBM and IT provider to review the monitoring and filtering systems and agree and record actions taken.

- receives reports from the Smoothwall system monthly which are reviewed and actions undertaken if necessary
- maintains an online filtering and monitoring incident log which records the nature of the incident, time and date reported and to whom, nature of any follow up action as well as the date of satisfactory resolution of the issue with signature
- ensures there are regular visits to review and test the filtering and monitoring systems made by the responsible governor and these are accurately recorded
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)
- receive regularly updated training to allow them to understand how digital technologies are used and are developing (particularly by learners) with regard to the areas defined In Keeping Children Safe in Education:
    - content
    - contact
    - conduct
    - commerce

3.4 Teaching and support staff

School staff are responsible for ensuring that:

- they understand that online safety is a core part of safeguarding.
- they have an awareness of current online safety matters/trends (DDSCP safeguarding updates, Derby School's circular etc.) and of the current school Online Safety Policy and practices.
- they have read, understood, and signed the staff acceptable use agreement (AUA)
- they immediately report any suspected misuse or problem to the headteacher for investigation/action, in line with the school safeguarding procedures
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- if an issue arises staff know to close the internet site down to prevent further viewing; however, the website history is not to be cleared until after it has been reported to the DSL. This may then need to be recorded on CPOMS.
- in lessons where internet use is pre-planned, it is best practice that 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
- where learners are allowed to freely search the internet, staff should be vigilant in supervising the learners and monitoring the content of the websites the young people visit
- where lessons (or activities e.g. transition meetings, live children's training, live assemblies) take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies as well as the guidance in Appendix 2.

- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc. All staff follow the relevant procedures and policies in place, including informing the DSL.
- 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. School staff should avoid having unrelated minors as their friends as part of good safeguarding practise.
- ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a ‘one size fits all’ approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

When using communication technologies, school employees are responsible for ensuring:

- any digital communication between staff and learners or parents/carers take place on school authorised platforms (e.g. e-mail, ClassDojo, etc.). This 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 the headteacher 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.

3.5 IT Provider

Whilst Wren Park employ LinkIT as their IT provider, it remains the responsibility of the school to ensure that the IT provider carries out all the online safety measures that the school’s obligations and responsibilities require. The IT provider follow and implement school Online Safety Policy and procedures.

The IT Provider is responsible for ensuring that:

- they are aware of and follow the school Online Safety Policy and all relevant policies 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 DfE Meeting Digital and Technology Standards in Schools & Colleges and guidance from Derby City 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/attempted misuse can be reported to the headteacher and DSL 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 systems are implemented and regularly updated as agreed in school policies

3.6 Learners

ZIP IT
Keep your personal stuff private and think about what you say and do online.
BLOCK IT
Block people who send nasty messages and don't open unknown links and attachments.
FLAG IT
Flag up with someone you trust if anything upsets you or if someone asks to meet you offline.

- Children are encouraged to discuss their online behaviour in open discussions and talk to staff.
- Within Upper Key Stage 2, the i- Vengers project is promoted, which involves completing tasks to help support the teaching of online safety and learn more about it to support other children. This serves to raise the prominence of the subject and gives the children pupil voice in the teaching and implementation of the subject. This group includes children with SEND which ensures they have a voice and their opinions are valued.
- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- are aware of the Online Safety motto: zip it, block it, flag it to an age appropriate depth
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so both at home and school
- know ways they can access support through school staff, worry boxes, and helplines (e.g. NSPCC)
- should know what to do if they or someone they know feels vulnerable when using online technology
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy and Behaviour Policy covers their actions out of school in line with the Keeping Children Safe in Education document.
- know how to use the British Values and the school values of being Respectful in the context of their online interactions

3.7 Parents and carers

We believe that parents play an integral part of keeping their children safe online and it is our role to support this. The school and teachers are open and approachable; therefore, encouraging parents to seek assistance and support. The school takes every opportunity to help parents and carers understand online safety and how to keep their children safe through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the learners' acceptable use agreement
- seeking their permissions concerning digital images, cloud services etc
- parents'/carers' evenings
- termly online safety newsletters
- website resources (including sections for SEND, transition to secondary and ways to access support)
- information about national/local online safety campaigns and literature

- Periodic opportunities to take part in face to face workshops with the Cyber Security section of the local police and online workshop with the NSPCC
- Pupils and parents will be informed of the complaints procedure; a copy of which is on the website
- targeted newsletters, resources and section of the website for parents of children with SEND

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to learners in school.
- inform the school of any personal devices brought into school so these can be kept safe until the end of school
- engaging with opportunities for information and workshops where possible
- working together to support children as they learn to negotiate the digital world. School will handle issues sensitively to support both parents and children

3.8 Community users

Community users (e.g. Premier Sports, Soccer Stars etc.) who access school systems as part of the wider school provision will be expected to sign a community user AUA before being provided with access to school systems and follow the online safety policy.

4. Educating pupils about online safety

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

All schools have to teach:

- Relationships education and health education in primary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous

- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

This is delivered through a carefully planned online safety curriculum for all year groups which is matched against a nationally agreed framework (including Education for a Connected World) and regularly taught in a variety of contexts.

Online safety is taught within the Jigsaw scheme in PSHE lesson as per the RSE policy; however, this is supplemented by the Teach Computing scheme which incorporates online safety in the context of the strands within computing. Alongside this, the Common Sense Education scheme has been chosen as a scheme to provide discrete lessons which ensure every child has the knowledge and skills to be safe and confident online. This is further supplemented by the Safer Internet Day and other opportunities.

- Lessons are matched to need; are age-related and progressively build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Learner need and progress are addressed through effective planning and assessment
- Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week
- the programme will be accessible to learners at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- learners should be helped to understand the need for the learner acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, with reference to the Computer Misuse Act 1990.
- staff should act as good role models in their use of digital technologies the internet and mobile devices
- the online safety education programme is relevant and up to date to ensure the quality of learning and outcomes.

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

4.1 Contribution of Learners

The school acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass learner feedback and opinion.
- appointment of i-Vengers to support and represent their peers
- learners contribute to the online safety education programme e.g. peer education, i-Vengers conducting surveys as well as planning and leading online safety campaigns
- learners designing/updating acceptable use agreements
- contributing to online safety events with the wider school community (Safer Internet Day)

This also ensures that the curriculum, policies and teaching are developed in conjunction with the children.

After careful consideration, Wren Park School has decided not to allow personal devices or technologies in the learning environment due to the following issues and risks which are felt to outweigh the benefits:

- security risks in allowing connections to your school network
- filtering of personal devices
- breakages and insurance
- access to devices for all learners
- avoiding potential classroom distraction
- network connection speeds, types of devices
- charging facilities
- total cost of ownership.

The school acceptable use agreements for staff, learners, parents, and carers outline the expectations around the use of mobile technologies.

4.3 Emotional Health and Well-being

Wren Park takes the well-being of the children seriously and has had many challenges and opportunities for children to have less screen time.

- Creative homework projects each term where children are encouraged to be outside, bake or make a craft item about that topic.

- Regular challenges to spend time at the weekend outdoors
- A campaign to turn off screen before bed (i-Vengers project)

5. Identify, intervene and escalate

Even the most vigilant school, staff or parent cannot eliminate risk in this ever changing fast paced area of development. It is not possible to “police” or prohibit such use of technology which clearly has a valuable place in the everyday lives of all children and adults. We aim to educate the children to become increasingly independent and adopt safe ways of using the internet positively. We are aware that there is a risk, which is ever changing, and we will support all children through encouraging them to seek the help of trusted adults should they be a victim of cyberbullying or if they feel uncomfortable with the material they encounter whilst using modern technology. We develop a culture where we foster and encourage children to feel safe in speaking freely about what they access electronically at school and home rather than to restrict and drive “underground” any potential areas of harm.

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:

Identify:

- Robust training to identify risks (categorised as the 4C’s) for all members of the school community
- Vulnerable children identified through the vulnerability tracker
- Specific risks for SEND children identified and parents educated about
- Open discussions and positive atmosphere to encourage children to talk about concerns
- Robust curriculum to ensure children are able to identify when they are uncomfortable and know what to do
- Parent workshops (face to face and virtual) to support parents to identify risks
- Parental trust and support to enable reporting
- Smoothwall provides age-appropriate filtering and monitoring which promptly creates alerts and reports

Intervene:

- Incidents are logged appropriately on CPOMS where there are specific categories to ensure patterns and trends (e.g. discrimination) are identified early as well as making it easy to analyse the types of incidents we are having. This also identifies and highlights incidents which are of a more serious nature.
- 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 are aware of the need to report online safety issues/incidents and how to do this.

- Reports will be dealt with as soon as possible as is practically possible once they received. This includes Veyon software which gives the ability to view and immediately lock a students computer from any teacher/ SLT laptop
- Smoothwall provides age-appropriate filtering and monitoring which promptly creates alerts and reports
- All members of staff are aware of their role and responsibilities to ensure all risks identified are evaluated and acted upon if necessary
- Reports will be dealt with as soon as is practically possible once they are received.

Escalate:

- The Designated Safeguarding Lead and other responsible staff have appropriate skills and training to make robust and effective decisions about how and where to escalate concerns
- Clear policies and procedures ensure incidents are escalated effectively and to the most appropriate organisation.
- Incidents are reflected upon to ensure they are learnt from and action is taken to safeguard all children.
- Through DDSCP, briefings and reports, the school is able to use the experiences and learning points from the local area and further a field to implement changes and learning points to further protect our children.
- 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, this may include
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

6. Responding to new and emerging risks

Wren Park Primary School recognises that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace. We will:

- carry out an annual review of our online safety approaches which will be supported by an annual risk assessment which considers and reflects the specific risks our pupils face.
- regularly review the methods used to identify, assess and minimise online risks.
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before their use is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that internet access is appropriate.
- recognise that due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our systems, and as such identify clear procedures to follow if breaches or concerns arise.

7. Professional standards and misuse

There is an expectation that required professional standards will be applied to online safety as in other aspects of school life i.e., policies and protocols are in place for the use of online communication technology between the staff and other members of the school and wider community, using officially sanctioned school mechanisms.

7.1 Staff

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 and the local authority.

Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff will be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- The procedure is conducted 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). The same device will be used for the duration of the procedure.
- The relevant staff have appropriate internet access to conduct the procedure, as well as the sites and content visited being closely monitored and recorded (to provide further protection).
- A record of the URL of any site containing the alleged misuse will be kept as well as a description of 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
- 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

- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively as well as being protected by the Whistleblowing Policy.

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.

- There are support strategies in place for those reporting or affected by an online safety incident
- Incidents are logged in the Online Filtering and Monitoring, Recording and Action Log (see Appendix 3)
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions
- learning from the incident (or pattern of incidents) will be provided anonymously:
  - for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
  - to staff, through regular briefings
  - to learners, through assemblies/lessons
  - to parents/carers, through newsletters, school social media, website
  - to governors, through regular safeguarding updates
  - to local authority/external agencies

7.2 Learners

Children are learning and will make mistakes. At Wren Park, we endeavour to support and educate children when this occurs so they can make different choices in the future (see relational behaviour policy). Where there is a concern about a child's online choices:

- the incident will be reported to the DSL and logged. The DSL will then decide what intervention is necessary and whether it needs escalating to an external agency.
- where the incident is considered serious, intentional or has been repeated, it may be necessary for the child to complete the learning without access to a computer to support them to rebuild trust before using the internet again
- parents will be informed if it is deemed appropriate
- any learning from the incident in terms of additional filtering, education for the class or age appropriately to the school or training for the school staff to address this will be completed.

8. Filtering, monitoring and security

The school is responsible for ensuring that the school infrastructure/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.

The school filtering and monitoring provision is agreed by senior leaders, governors and the IT Provider and is regularly reviewed (at least annually) and updated in response to changes in technology and patterns of online safety incidents/behaviours The school Internet access will be designed expressly for children's use and will include filtering appropriate to the age of pupils. Filtering is provided though Smoothwall system.

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. The DSL has lead responsibility for safeguarding and online safety and the IT service provider will have technical responsibility.

- The filtering and monitoring provision is reviewed (at least annually) by senior leaders, the Designated Safeguarding Lead and a governor with the involvement of the IT Service Provider. checks on the filtering and monitoring system are carried out by the IT Service Provider with the involvement of a senior leader
- The Designated Safeguarding Lead and a governor, in particular where a safeguarding risk is identified, there is a change in working practice

8.1 Filtering

The school manages access to content across its systems for all users and on all devices using the Smoothwall. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges.

- Smoothwall is a member of the Internet Watch Foundation (IWF) which provides an up-to-date URL list which helps ensure access is blocked to illegal child abuse images and content.

- They also use the police assessed list of unlawful terrorist content, produced and updated on behalf of the Home Office to ensure terrorist content is blocked.

- Inappropriate content is also blocked. This includes:
  - Discrimination against the protected characteristics: Any form of prejudice on grounds of race, religion, age, sex, disability, marriage or sexual orientation.
  - Drugs/substance abuse: Anyone displaying or promoting the illegal use of drugs or substances.
  - Extremism: Anyone promoting terrorism and terrorist ideologies, violence or intolerance.
  - Malware/hacking: Any form of compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content.
  - Pornography: Displays of sexual acts or explicit images.
  - Piracy and copyright theft: Illegal provision of copyrighted material.
  - Self-harm: Promotion or display of deliberate self-harm (including suicide and eating disorders).
  - Violence: Any display or promotion of the use of physical force intended to hurt or kill.

  The filter system has different levels of user so that staff logins are not over blocked which would disrupt teaching and learning; however, children are only able to access age-appropriate sites.

- It is accepted that from time to time, for good educational reasons, students may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need. This should be time limited and regularly reviewed.

- There are established and effective routes for users to report inappropriate content with children knowing how to 'Flag it,' and adults aware of their reporting responsibilities. However, it is recognised that no filtering system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes
- filtering logs are regularly reviewed and alert the Designated Safeguarding Lead to breaches of the filtering policy, which are then acted upon.
- the school policy on mobile phones is that they are accessed in staff areas only and are not using wi-fi without permission for an agreed and time limited reason.
- access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

If necessary, the school will seek advice from, and report issues to, the SWGfL Report Harmful Content site.

8.2 Monitoring

The school uses Smoothwall monitoring systems to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored. This enables effective and swift identification which enables the DSL to intervene in a timely and efficient manner; therefore, concerns can be escalated appropriately if required.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and good practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment. These include:

- physical monitoring (adult supervision in the classroom)
- Veyon software enables adults to monitor all screens at once, as well as to lock screens if there is an online safety breach
- internet use is logged, regularly monitored and reviewed by a team comprising of the SBM, DSL and IT provider
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention
- filtering logs are regularly analysed and breaches are reported to the DSL

- school technical staff regularly monitor and record the activity of users on the school technical systems

8.3 Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements. The responsibility for technical security resides with SLT who may delegate activities to identified roles.

- 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 IT service provider and will be reviewed, at least annually, by the SLT
- All users have an individual login which supports filtering and monitoring but also security. Users must not allow other user to use their account (including staff using children's and children using member of staff's)
- Password policy and procedures are implemented (consistent with guidance from the National Cyber Security Centre)
- All users 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.
- All school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- The administrator passwords for school systems are kept in a secure place, e.g. school safe.
- There is a risk-based approach to the allocation of learner usernames and passwords.
- 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
- 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 software.
- There are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- LinkIT 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 (report to the school business manager or computing lead) is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed
- Use of school devices out of school and by family members is regulated by an acceptable use statement that a user consents to when the device is allocated to them
- Personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network

- Staff members should not install software on a school-owned devices without the consent of the IT service provider. This requires the administrator password.
- Systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- Mobile device security and management procedures are in place
- Guest users are provided with appropriate access to school systems based on an identified risk profile. Supply teachers have a specific login which has appropriately limited access to school systems and prevents breaches of data and confidentiality.

9. School communication

9.1 Text messaging

Parents are contacted using Teachers2Parents.co.uk. Mobile numbers are online and protected by a SSL 128 bit certificate. This is the same protection technology used by online banking. All of their staff are DBS checked and the company is fully registered with the data protection register.

New parents will be asked for their details when their child starts school. Any undelivered messages will be followed, up as this may mean incorrect numbers or full mailboxes.

The school also uses Class Dojo as a method of communication; however, this is not always checked regularly. Class Dojo is compliant with GDPR (see safety and privacy). In further compliance with GDPR, children's full names are not used and parents choose to create an account and the amount of information they provide. This is used to exchange work and communicate with parents. Parents are encouraged to contact the school using email and phone calls for confidential matters. Children have their own account through which they can submit work and make comments on the class and school story which is monitored by school staff. There is no facility for the children to contact other students through Class Dojo.

9.2 Publication of pupil's images or work

- Staff will ensure that only digital cameras and ipads provided by the school will be used to photograph pupils. Staff should not use personal mobile phones to take photographs of children, except with the specific approval of the headteacher for a reason which will be time limited and purpose to be agreed.
- Staff will ensure that all photographs of pupils are deleted from the school digital cameras as soon as practically possible once transferred.
- Staff will ensure that no photograph or image of pupils will be transferred to personal or home computer systems this also includes personal USB devices.
- The school operates an 'opt out' policy for photograph permissions. Pupil's photographs may be published on the school website, unless parents have opted out upon admission to school. (School will be vigilant in particular cases where a child is viewed as vulnerable- safe and secure knowledge of these children is known by website administrator).
- Pupils' full names will not be used anywhere on the school web site or other unsecured on-line space.

- Work can only be published with the permission of the pupil and parents/carers.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic hardware upon admission to school.

9.3 Management of social networking and personal publishing

- The Smoothwall system will block access to social networking sites for all users
- Newsgroups are blocked unless a specific use is approved.

10 Social media

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

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

School staff should ensure that:

- no reference should be made in social media to learners, 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

10.3 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 on, 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, or the reputation of a person working for the school or the reputation of the school are outside the scope of this policy
- where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- the school permits reasonable and appropriate access to personal social media sites during school hours; however, this should be during off duty times, within a staff only area and for viewing online. The posting of social media comments during school times is not permitted as these could be construed as being the opinions of the school.

10.2 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 best practise and careful thought about each incident, in line with other policies which may be relevant
- 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.

In the event of any social media issues that the school is unable to resolve, support may be sought from the Professionals Online Safety Helpline.

10.3 Digital and video images

The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- the school may use live-streaming or video-conferencing services in line with national and local safeguarding guidance / policies.
- when using digital images, staff will inform and educate learners about the risks associated with the taking, use, sharing, publication and distribution of images.
- staff/volunteers must be aware of those learners whose images must not be taken/published. Those images should only be taken on school devices. The personal devices of staff are not be used for such purposes
- in accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, parents are reminded at each event that these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *learners* in the digital/video images
- care should be taken when sharing digital/video images that learners are appropriately dressed
- learners must not take, use, share, publish or distribute images of others without their permission
- photographs published on the website, or elsewhere that include learners will be selected carefully and will comply with Online Safety Policy
- learners' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- 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

10.4 Online Publishing

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

- Public-facing website
- Class Dojo
- School newsletters
- School newspaper
- SEND and termly online newsletter

The school website is managed/hosted by Primary Sites. The school ensures that 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 learner work, images or videos are published, their identities are protected, and full names are not published. Wren Park Primary School operates an 'opt-out' to allow parental choice about the use and sharing of their child's image.

11 Data Protection

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

The school:

- 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) who has effective understanding of data protection law and is free from any conflict of interest.
- 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
- 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, volunteers, teenagers, and older children with information about how the school looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- 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 (below) 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. Staff have access to Onedrive and Sharepoint to be able to work effectively at home; however, with regard to staff well-being this is as limited as possible and not encouraged beyond what is necessary
- 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.

11.1 School owned/provided devices

- all school devices are managed though the use of Mobile Device Management software
- there is an asset log that clearly states whom a device has been allocated to. There is clear guidance on where, when and how use is allowed
- personal use (e.g. online banking, shopping, images etc.) is clearly defined and expectations are well-communicated.
- the use of devices on trips/events away from school is clearly defined and expectation are well-communicated.
- liability for damage aligns with current school policy for the replacement of equipment.
- education is in place to support responsible use.

11.2 Communicating the Policy

Introducing the policy to pupils

- Pupils will be informed that network and Internet use will be monitored.
- An online safety training programme will be introduced to raise the awareness and importance of safe and responsible internet use.
- Instruction in responsible and safe use should precede internet access.
- Online safety is included within Computing and also the Jigsaw scheme which covers the use of technologies safely when both in school and at home
- Regular whole assemblies are held by the Computing coordinator / senior staff to highlight the importance of e safety and the latest risks.

Introducing the policy to parents

- Parents will receive an acceptable use policy
- The policy will be advertised by the newsletter, the online safety newsletter as well as email with a link

- The policy will be available on the school website

Introducing the policy to staff

- The headteacher will ensure all staff have read and understood the policy and are compliant with it

Outcomes

The impact of the Online Safety Policy and practice is regularly evaluated through the review/audit of online safety incident logs; behaviour/bullying reports; surveys of staff, learners; parents/carers and is reported to relevant groups:

- there is balanced professional debate about the evidence taken from the reviews/audits and the impact of preventative work e.g., online safety education, awareness, and training
- there are well-established routes to regularly report patterns of online safety incidents and outcomes to school leadership and Governors
- parents/carers are informed of patterns of online safety incidents as part of the school's online safety awareness raising
- online safety (and related) policies and procedures are regularly updated in response to the evidence gathered from these reviews/audits/professional debate
- the evidence of impact is shared with other schools, agencies and LAs to help ensure the development of a consistent and effective local online safety strategy.
- However, the main outcome of this policy is that children at Wren Park Primary School are as safe as possible when using devices both at home and school through robust polices and procedures but also effective relationships throughout the school community. Children and their families are given information, tools and support to keep all children (especially our more vulnerable children) as safe as possible in the ever-changing digital world.

IMPORTANT UPDATE JAN 2025
Regarding the use of AI in school.

Over very recent times there has been a massive increase in the use of Artificial Intelligence (AI) in business, commerce and within personal / domestic use. Education is not immune to these advances and it is an exciting time in terms of opportunities for education and within the curriculum taught to children but legislation and National guidance for use of AI in schools is not yet in place.

Within Wren Park we wish to utilise and benefit from such advances in technology but are also aware of potential risks in broad terms under the umbrella of Safeguarding children. We will be keeping abreast of advances in AI and working through exploring opportunities and reducing risks for its successful and effective use within school, within the curriculum and within children's experiences. We will be looking at the skills we need to equip children and staff with to use AI safely.

In broad terms, our approach has been to establish a baseline of staff understanding of the uses of AI (Jan 25) and highlight the guidance that staff need to be aware of in terms of safe use of technology in relation to:

- KCSIE 24

- PREVENT DUTY & British Values
- Working Together to Safeguard Children 23
- GDPR
- Staff Code of Conduct
- Safeguarding and Child Protection Policy
- Online filtering and monitoring

HT has provided staff with some initial general guidance around sensible use of AI at this time including:

- As a teacher aid for adapting / creating lesson resources eg. powerpoints, pictures, worksheets
- To create resources such as story openers, character descriptions or success criteria and WAGOLL (What A Good One Looks Like).
- To assist teachers with report writing comments (further detail to be given around Easter)
- To assist with tasks such as letters to parents, curriculum document (starting prompts to be professionally adapted).

At this time we have taken the decision not to allow children to use AI within their own learning at school until we have appropriate rules and safeguards in place.

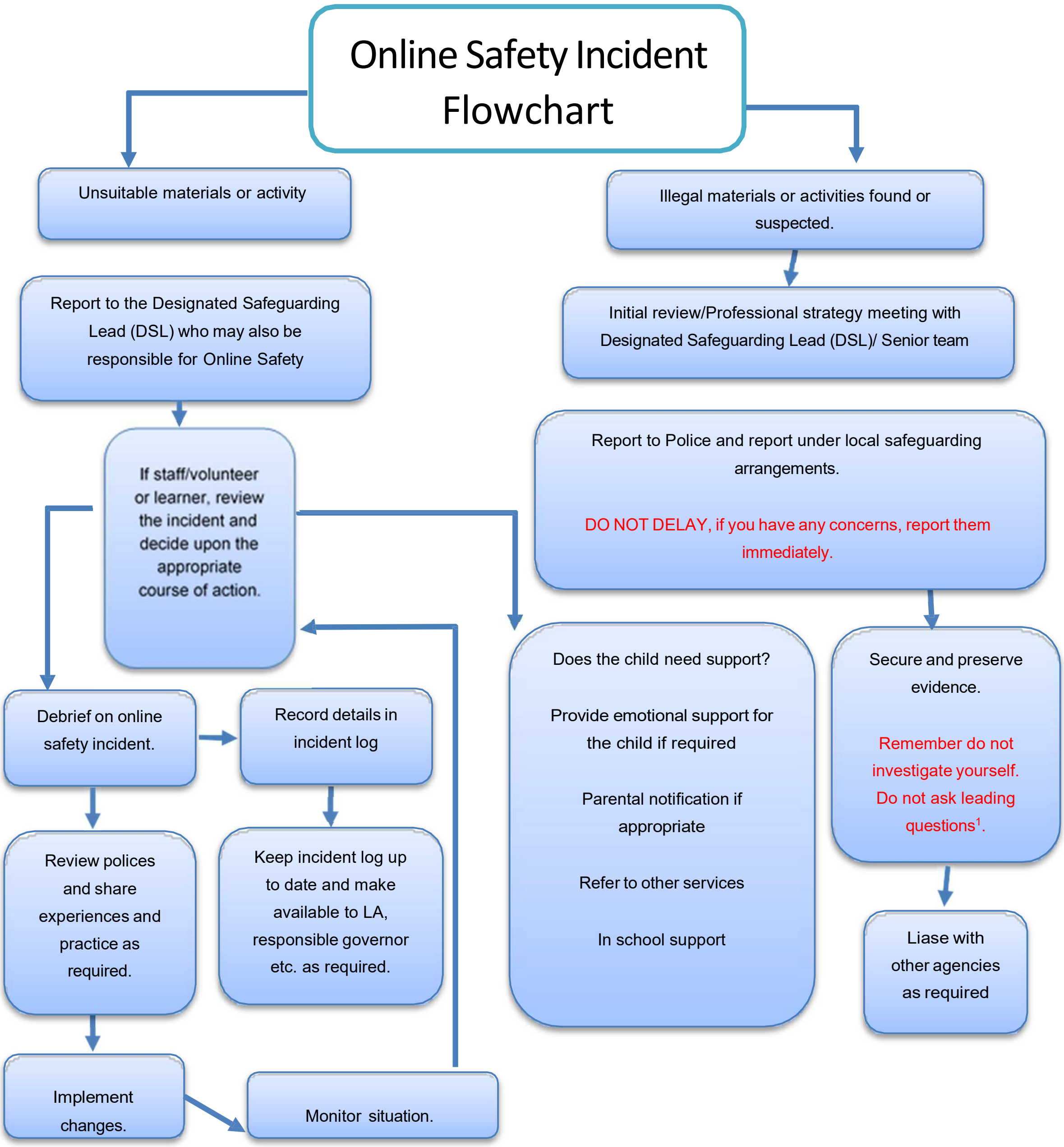
However, a member of staff may input a child's work / ideas to AI for a valid reason (eg. Write their story, character description to create a further visual stimulus, word bank or other resource) but, the member of staff must ensure that this is not viewed by the child until it has been vetted as suitable.

NEXT STEPS
The Headteacher will be taking the lead within this area this year and will undertake the following:

- Staff CPD/ Professional discussions sharing "good AI" tools for teachers (at least termly).
- Attend any relevant CPD and cascade this to staff.
- Work with Safeguarding governor and Teaching and Learning committee to look at issues.
- To consider where AI may fit effectively with the Computing Curriculum and other subject areas.
- Seek further guidance from networks and colleagues within LA schools and beyond.
- Work with i-Vengers to establish children's use of AI
- Provide some helpful guidance for parents on keeping children safe when using AI at home
- Provide some guidance for children around being critical thinkers through some activities eg. Responding to AI generated images or text.
- Subject leads to consider how AI may be used to enhance aspects of their subject (but not yet action)
- HT to oversee any small scale "pilot project" of children using AI which may take place as part of our "sensible and safe" embracing of AI. To liaise with governors, staff and parents should this be started within the 2025-26 year.

Appendix 1

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



Online Safety Incident Flowchart

Unsuitable materials or activity

Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety

If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.

Debrief on online safety incident.

Record details in incident log

Review polices and share experiences and practice as required.

Keep incident log up to date and make available to LA, responsible governor etc. as required.

Implement changes.

Monitor situation.

Illegal materials or activities found or suspected.

Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team

Report to Police and report under local safeguarding arrangements.

DO NOT DELAY, if you have any concerns, report them immediately.

Does the child need support?

Provide emotional support for the child if required

Parental notification if appropriate

Refer to other services

In school support

Secure and preserve evidence.

Remember do not investigate yourself. Do not ask leading questions[1].

Liase with other agencies as required

The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

Appendix 2

Managing Information Systems

Information systems security

Local Area Network security issues:

- Users must act reasonably – e.g. the downloading of large files during the working day will affect the service that others receive.
- Workstations are secured against user mistakes and deliberate misuse.
- The server operating system is secured and kept up to date.
- Virus protection and Firewall services for the whole network is installed and updated regularly by Link IT

Wide Area Network (WAN) security issues:

- Personal data will only be sent over the Internet by secured school email addresses.
- Personal carried on portable media will be encrypted or otherwise secured.
- Portable media may not be used by pupils without specific permission followed by a virus check. Staff may use portable media. They must be encrypted.
- Files held on the school's network will be regularly checked.
- The Computing co-ordinator Link IT will review system capacity regularly.

Management of Videoconferencing

The Equipment and Network

- ➢ Videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- ➢ All videoconferencing equipment in the classroom must be switched off when not in use and not set to auto answer.
- ➢ Equipment connected to the educational broadband network should use the national E.164 numbering system and display their H.323 ID name.
- ➢ External IP addresses should not be made available to other sites.
- ➢ Videoconferencing contact information is not put on the school Website.
- ➢ Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- ➢ Videoconferencing should be supervised appropriately for the pupils' age.
- ➢ Parents and guardians should agree for their children to take part in videoconferences.
- ➢ Only key administrators should be given access to the videoconferencing system, web or other remote control page available on larger systems.
- ➢ Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.
- ➢ When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.
- ➢ If third-party materials are to be included, check that recording is acceptable to avoid infringing the third-party intellectual property rights.

- Videoconferencing is a challenging activity with a wide range of learning benefits. Preparation and evaluation are essential to the whole activity.
- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material that is appropriate for your class.
- During the pandemic, Microsoft Teams was used for well-being sessions during lockdowns and whole class isolations. This is used under parental supervision following the safeguards in place through Wren Park's Microsoft Teams Virtual Classroom Agreement. When children use Microsoft teams in school, it is done so under the direct supervision of an adult with parental consent if it is to a person outside of Wren Park (e.g. secondary schools for transition).