Rosehill School

E-Safety Policy

Date of policy:	September 2023 Updated January 2024
Policy Leads:	Policy Writer - Headteacher Policy Lead - Computing Lead
Date of approval:	Full Governing Body Meeting 7.2.2024
Date of next review:	September 2024

Contents:

Statement of intent

Rosehill School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. We believe that technology can provide: enhanced collaborative learning opportunities; better engagement of pupils; easier access to rich content; support conceptual understanding of new concepts and can support the needs of all our pupils.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils 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, fake news, 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.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils 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 pupils and staff.

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2021'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- DfE (2024) Filtering and Monitoring Standards for Schools and Colleges guidance

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Information Filtering and Monitoring Policy
- Allegations of Abuse Against Staff Policy
- GDPR Data Protection Policy
- GDPR Data Incidents and Breaches Policy
- Child Protection and Safeguarding Policy
- Pupil Friendly Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSHE Policy
- Staff Code of Conduct
- Positive Behaviour Support and Physical Intervention Policy
- Disciplinary Policy
- Staff and Volunteer Confidentiality agreement
- Photography Policy
- Remote Learning Policy
- Pupils IDevices Policy- Including Pupil Acceptable Use Agreement
- Staff ICT and IDevices Policy- Including Staff Acceptable Use Agreement

2. Roles and responsibilities

The governing board 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 induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.
- To support the school in encouraging parents and the wider community to become engaged in online safety activities.

The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the Computing Lead by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents and carers to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the Computing Lead and ICT technician to conduct termly light-touch reviews of this policy.
- Working with the Computing Lead and governing board to update this policy on an annual basis.
- Ensuring all E-Safety incidents are dealt with promptly and appropriately in line with school policy.
- To be aware of procedures to be followed in the event of a serious online safety incident.

The Computing Lead is responsible for:

- Taking the lead responsibility for online safety in the school.
- Ensure that online safety is embedded within the curriculum.
- Acting as the named point of contact within the school on all online safeguarding issues- referring issues to a DSL, as required.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. IT technician.
- Ensuring online safety is considered within the school's approach to remote learning.
- Keeping up-to-date with current research, legislation and online trends.

- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Working with DSLs to establish a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff. Ensuring all members of the school community understand the reporting procedure.
- Reporting to the governing board about online safety on an annual basis.
- Monitor the effectiveness and impact of the Digital Safety policy and curriculum across school, reporting back to staff and governors.
- Working with the headteacher and IT technician to conduct termly light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an annual basis.
- Engage with parents and school community regarding E-Safety matters, including updating regularly the E-Safety pages of the website with the most current advice and work from the children.

The DSL is responsible for:

- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Computing Lead.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Working with the Computing Lead in establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Working with the headteacher, Computing Lead and IT technician, where required, to conduct termly light-touch reviews of this policy.
- Ensuring that the school's filtering and monitoring systems are updated and reviewed regularly.

IT technician is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated and reviewed regularly.
- Ensure filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the Lead DSL and Computing Lead.
- Working with the Computing Lead and headteacher to conduct termly light-touch reviews of this policy.

SCHOOLS IT technical support:

- Provide a technical infrastructure to support E-Safety practices.
- Ensure the IT technical infrastructure is secure and the network and server are secure.
- Ensure the anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Ensure Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Ensure any E- Safety technical solutions such as Internet filtering are operating correctly.
- Passwords for staff will be a minimum of 8 characters (and will be alphanumeric).
- Two factor authentication is set up on all staff emails.
- The IT System Administrator password is to be changed on a monthly (30 day) basis and is only kept by IT support not staff members.
- That the use of school technology and online platforms are regularly monitored and that any misuse/attempted misuse is reported to the Headteacher.
- They will also work with the senior leadership team and Lead DSL to procure systems, identify risk, carry out reviews and carry out regular checks.

All staff members are responsible for:

- Taking responsibility for the security of IT systems and electronic data they use or have access to.
- Ensure the safe use of devices by all pupils and ensure pupils are supervised at all times.
- Deal with E - Safety issues as soon as they become aware of them and know how to report concern or incidents to the Lead DSL in line with the school's reporting procedure.
- Develop an awareness of E- Safety issues and how they relate to pupils in their care, including undertaking training delivered in school.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.
- Adhere to acceptable use policies and the Staff Code of Conduct.

Pupils are responsible for:

- Adhering to the Acceptable Use Agreement and other relevant policies.
- 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 and the schools Pupil Friendly Safeguarding Policy.

3. About our school and pupils

Rosehill School is a special school for children and young people (aged 4-19), on the autism spectrum. The pupils attending the school have a range of overlapping needs in addition to autism, including physical, sensory, medical and behavioural needs. Autism is a lifelong disability; the characteristics of autism vary from one person to another, but there are some main areas of difference, and the very large majority of children and young people attending the school will have a range of abilities and needs within each of these areas:

- **Communication:** Differences in understanding and expressing communication and language, with skills ranging from individuals who are highly articulate, to others who may be non-verbal,
- **Social understanding:** Differences in understanding social behaviour and the feelings of others, which informs the development of friendships and relationships;
- **Interests and information processing:** Differences in perception, planning, understanding concepts, generalising, predicting, managing transitions, passions for interests and ability to absorb auditory or spoken information;
- **Sensory processing:** Differences in perceiving sensory information. Hypo (low sensitivity), hyper (high sensitivity), touch, sight, hearing, smell, taste, vestibular inner ear (balance), proprioceptive (body awareness).

Through ongoing feedback from children, young people and families, and in addition to training and research, the school is aware that for many adults and children on the autism spectrum they can feel that it is not their autism that poses them difficulties as such, but the expectations and/or responses they can have from other people. In particular, the expectation to act, respond and learn in the same way that more typically developing peers do.

When working with pupils at Rosehill, we ensure that all staff who work with the children and young people enhance their understanding of these differences and make adjustments to their own style of interaction and their expectations and modify how they interact and deliver the curriculum to our pupils. For example, being aware of the differing ways that learners process information, and therefore providing personalised responses/ interventions and support.

This Policy and the Schools Computing, RSE and ESafety Curriculum content pays due regarding to the needs of the pupils attending the school, and 'Schemes of Work' and 'Subject Pathways' (age and stage appropriate content), are adapted, tailored and where appropriate personalised, to support individual needs.

4. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The Computing Lead has overall responsibility for the school's approach to online safety, with support from the headteacher and Senior Leadership Team where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies are conducted on the topic of remaining safe online
- The school takes part in ESafety activities and events
- The school invites visitors into the school who support safe use of the internet

Handling online safety concerns

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Child Protection and Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the Computing Lead or a DSL, who investigates concerns with relevant staff members, e.g. the headteacher and IT technician, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Positive Behaviour and Physical Intervention Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by a DSL.

5. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom

- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

6. Peer-on-peer sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school and off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Child Protection and Safeguarding Policy.

7. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- The pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- The pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.

- The pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- Talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- The pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The Computing Lead, in conjunction with DSLs, will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

- Being secretive about how they are spending their time.
- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to a DSL without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the Headteacher/ DSL without delay, who will handle the situation in line with the Prevent Duty Policy and Child Protection and Safeguarding Policy.

8. Mental health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The Computing Lead will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the school wellbeing procedures and the Child Protection and Safeguarding Policy.

9. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to a DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the Computing Lead, DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.

- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or even to individual children at risk where appropriate.

The Computing, DSLs and headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

10. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The Computing Lead, DSLs and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

11. Online safety training for staff

The DSLs will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that

pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, and the Child Protection and Safeguarding Policy.

12. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:

- RSE
- Health education
- PSHE
- Citizenship
- Computing and IT

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Why the internet is important

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Internet use is part of the statutory curriculum and a necessary tool for learning.

Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security. Information will be provided to parents about how to educate and support their children with safe internet use.

Internet use will enhance learning

- The Internet is an essential element in 21st century life for education, business and social interaction. The school recognises it has a duty to provide pupils with high-quality internet access as part of their learning experience in school and prepare them to make safe and effective use out of school.
- The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff will guide pupils in online activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be taught to become responsible, respectful and competent users of data, information and communication technology.
- Pupils will be equipped with skills, strategies and knowledge that will enable them to reap the benefits of the online world, whilst being able to minimise the risk to themselves or others.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to keep themselves safe online
- What healthy and respectful relationships, including friendships, look like
- Consent, e.g. with relation to the sharing of personal information
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix A of this policy.

The Computing Lead take the lead on the development of the school's online safety curriculum, supported by the DSLs and Headteacher. Pupils and parents/carers will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites that the pupils use and the kinds of behaviours in which they engage with online.

The school recognises that, all pupils attending Rosehill School are vulnerable online, and there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online. The DSLs and designated teacher for LAC, will work with the Computing Lead to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school takes a more personalised and contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they autism friendly?
- Are they appropriate for pupils' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Computing Lead, supported by the Headteacher, will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The Computing Lead, with advice from DSLs as required, will advise the class teacher on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully to support all pupils needs.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

13. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age, ability and needs.

14. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Acceptable Use Agreement for Pupils (supported by parents/ carers).

Staff and pupils will use all smart technology and personal technology in line with the school's IDevices Policy.

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

The school will hold assemblies and lessons, where appropriate, to support the safe use of smart technology and outline the importance of using smart technology in an appropriate manner.

The school will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4C's (content, contact, conduct and commerce) when educating pupils and supporting parents and carers to understand the risks involved with the inappropriate use of smart technology.

The school will support parents and carers in implementing appropriate and safe use of smart technology, as outlined below.

15. Educating parents/carers

The school works in partnership with parents and carers to ensure pupils stay safe online at school and at home. Parents/carers are provided with information about the school's approach to online safety and their role in protecting their children. Parents/carers are sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child, as appropriate.

Parents/carers will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents/carers workshops and training sessions
- Newsletters and information sharing
- Online resources
- The school's website https://www.therosehillschool.com/e-safety/

16. Internet access

Staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure ind

Filtering and monitoring online activity

Currently, the school use Smoothwall filtering and monitoring systems. DSLs will get weekly monitoring reports of student accounts from Smoothwall and any safeguarding concerns will be flagged immediately.

The governing board ensures the school's ICT network has appropriate filters and monitoring systems in place. The governing board ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The headteacher, School Business Manager and IT technician undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. The IT technician undertakes half-termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Any changes made to the system are recorded by School Business Manager and IT technician. Reports of inappropriate websites or materials are made to an IT technician immediately, who investigates the matter and makes any necessary changes. This will be recorded by the School Business Manager and IT Technician.

Deliberate breaches of the filtering system are reported to a DSL and IT technician, who will escalate the matter appropriately. If a pupil or staff has deliberately breached the filtering system, this will be managed in line the appropriate policy.

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 are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSLs who manage the situation in line with the appropriate policies.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT technician. Firewalls are switched on at all times. The IT technician reviews the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the IT technician.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils in Key Stage 4 and 5, where appropriate, are provided with their own unique

username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will be changed regularly to ensure security is maintained.

Users should inform the IT technician if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the headteacher is informed and decides the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

18. Emails

Access to and the use of emails is managed in line with the GDPR and Data Protection Policy, Acceptable Use Agreements, and the Staff and Volunteer Confidentiality Policy.

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

Staff members (and pupils, as supported by staff) are required to block spam and junk mail, and report the matter to the IT technician. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils (as appropriate) are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

The IT technician will update staff, regarding what a phishing email and other malicious emails might look like.

Any cyber-attacks initiated through emails are managed in line with the GDPR Data Incidents and Breaches Policy.

19. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time.

Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive annual training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents/carers over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents/carers are not able to contact them on social media. Where staff have an existing personal relationship with a parent/carer or pupil, and thus are connected with them on social media, e.g. they are friends with a parent/carer at the school, they will disclose this to the headteacher and will ensure that their social media conduct relating to that parent/carer is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online ESafety curriculum. Pupils will be taught about personal safety when using social networking sites outside the school and advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Concerns regarding the online conduct of any member of the school community on social media are reported to the headteacher/DSLs and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for official educational or engagement purposes. Staff members must be authorised by the headteacher to access to the school's social media accounts.

All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.

20. The school website

The headteacher, with support from the IT Technician and Computing Lead, is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the provisions in the Photography Policy are met.

The school has sought parental consent for any images of children that are used on the school website. To ensure the children's safety only first names will be published on the site, particularly in association with photographs.

21. Use of devices

School-owned devices

Staff members are issued with the following devices to assist with their work:

- Laptops
- Tablets
- iPods and Earwig devices (assessment devices)

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected, retrieved or erased.

The IT technician will review all school-owned devices on an ongoing basis, as required, to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from the Computing Lead and IT technician.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Positive Behaviour Support and Physical Intervention Policy respectively.

See the schools iDevices Policy for further information.

22. Personal devices

Any personal electronic device that is brought into school is the responsibility of the user.

The school implements a "Phone-Free School" Campaign (Appendix B).

Personal devices are not permitted to be used in the following locations:

- Pupils learning areas
- Toilets/ Changing rooms

Staff members, including supply staff, are not permitted to use their personal devices during lesson time, other than in an emergency (as advised by the headteacher within the school's emergency procedures training). Staff members are not permitted to use their personal devices to take photos or videos of pupils.

Staff members should report any concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

Pupils are not permitted to use any personal devices during lesson time.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the Headteacher/Senior Leadership Team.

23. Remote learning

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

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/ carers 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/carers to:

- Reinforce the importance of children staying safe online.
- Ensure parents/carers 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/carers 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.

24 Communication

24.1 Introducing the E- Safety Policy to pupils

- All pupils will be taught about digital safety regularly and will help to design posters about safety rules.
- E- safety rules will be displayed in rooms with Internet access.
- Pupils will be informed that network and Internet use will be monitored.
- Pupils will engage in the annual safer internet day alongside focussed work of different aspects of e-safety in computing and PSHE sessions.
- Instruction in responsible and safe use should precede Internet access.

24.2 Staff and the Digital Safety Policy

- The E- Safety Policy and its application and importance will be discussed and approved by all staff.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretions and professional conduct are essential.
- Staff understand the importance of identifying, intervening in and escalating any concerns regarding content, contact, conduct and commerce as stated in the Keeping Child Safe in Education guidance.
- Staff understand the appropriateness of use of their own personal devices such as smart phones and watches as detailed in the Staff Code of Conduct. Staff are provided with an earwig phone to use for taking photographs of children's work and engagement with learning.

24.3 Parental Involvement

- Internet use (including online gaming) in pupils' homes is increasing rapidly. Unless parents are aware of the dangers, pupils may have unrestricted access to the Internet.
- Parents' attention will be drawn to the school's E- Safety Policy in newsletters, the school prospectus and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged and guidance on Internet use in the home will be issued.

24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the Computing Lead, DSLs, IT technician and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and Computing Lead, with input from DSLs and the IT Technician, review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2024.

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

Appendix A: Online harms and risks – curriculum coverage

The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. Rosehill has used this information to assist in developing its own online safety curriculum; also, in line with local needs and the needs of our pupils. It is important to note, that the information in the 'curriculum areas' column is a guide, and will be tailored/personalised/amended to suit the needs of the pupils/individuals, as required. For further information regarding all aspects, please view the schools Computing and RSHE Curriculum.

Subject area	Description and teaching content recommended by the DfE	Curriculum area at Rosehill will aspects of this content will be covered, as appropriate to the pupils
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Misinformation and being aware that false and misleading information can be shared accidentally • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • How to keep safe online • The potential consequences of sharing information that may not be true	This risk or harm is covered in the following curriculum areas: • KS1/2- Relationships and health education • KS3-5- RSE • KS2-5-Computing • KS3/4- Citizenship
Fake websites and scam emails	Fake websites and scam emails are used to obtain data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: • How to recognise fake websites • The risks of entering information to a website which is not secure	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Computing

	• What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: • What identity fraud, scams and phishing are • That children are sometimes targeted to access adults' data • What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • How to recognise phishing scams • The importance of online security to protect against viruses that are designed to gain access to password information • What to do when a password is compromised or thought to be compromised	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: • How and why personal data is shared by online companies • How pupils can protect themselves and that acting quickly is essential when something happens • The rights children have with regards to their data • How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: • Health education • Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: • How to find information about privacy settings on various devices and platforms • That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: • How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts • How the targeting is done	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing

	• The concept of clickbait and how companies can use it to draw people to their sites and services	
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal. Teaching includes the following: • The types of online abuse, including sexual harassment, bullying, trolling and intimidation • When online abuse can become illegal • How to respond to online abuse and how to access support • How to respond when the abuse is anonymous • The potential implications of online abuse • What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: • KS1-2- Relationships education • KS3-5- RSE • Health education • Computing • KS4/5- Citizenship
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: • What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal • How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why • That it is okay to say no and to not take part in a challenge • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: • That online content (sometimes gang related) can glamorise the possession of weapons and drugs • That to intentionally encourage or assist in an offence is also a criminal offence • How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: • That, in some cases, profiles may be people posing as someone they are not • How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE • Health education • Computing
Grooming	Knowing about the different types of grooming e.g. radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: • Boundaries in friendships with peers, in families, and with others • Key indicators of grooming behaviour	This risk or harm is covered in the following curriculum areas: • KS1-2- Relationships education • KS3-5- RSE

	• The importance of disengaging from contact with suspected grooming and telling a trusted adult • How and where to report grooming both in school and to the police	
Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • That pupils should not feel pressured to do something online that they would not do offline • Why people sometimes do and say things online that they would never consider appropriate offline • The risk of watching videos that are being livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming	This risk or harm is covered in the following curriculum areas: • KS3-5- Health education
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: • That pornography is not an accurate portrayal of adult sexual relationships • That viewing pornography can lead to skewed beliefs about sex and, in some circumstances • That not all people featured in pornographic material are doing so willingly	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm is covered in the following curriculum areas: • KS1-2- Relationships education • KS3-5- RSE • Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: • KS3-5- Health education
Impact on quality of life, physical and mental health	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following:	This risk or harm is covered in the following curriculum areas: • Health education

and relationships	• How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum areas: • KS3-5- RSE
Self-harm	Pupils may raise topics including self-harm. Teachers must be aware of these risks.	

Appendix B: Our "Phone-Free School" Campaign

Rosehill School

Our "Phone-Free School" Campaign

Dear parents, carers and other members of the school community,

At Rosehill School we have been working hard to ensure that anyone coming onto the school site respects and follows our no mobile phone policy in order to safeguard the children and young people attending the school.

This policy means that no mobile phones can be used in any part of the school, including the front of school and reception area.

The Student Council have been regularly checking the implementation of this policy; staff and pupils will continue to enforce this policy, by reminding everybody of this campaign.

Last year, the Student Council ran a no mobile phone poster competition. The Chair of the Student Council chose the winning poster and this can be found on our safeguarding display in our school reception. The poster was created by pupils in the Primary School.

When coming into Rosehill School, you will be reminded about these procedures.

Thank you for your support

Rosehill Student Council